DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

The Honorable Carolyn N. Lerner
Special Council
U.S. Office of Special Counsel
1730 M. Street, N.W., Suite 218
Washington, DC 20036-4505

Dear Ms. Lerner,

Thank you for your letter requesting an investigation of alleged security violations at the Strategic Systems Program (SSP) Headquarters, located on the Washington Navy Yard (OSC DI-13-2348 and DI-13-2309). The Secretary of Defense expressly authorized me to send this report on his behalf per 5 U.S.C 1213 (d).

Enclosed is the report of the investigation led by the Naval Inspector General (NAVINSGEN). The inquiry found that there were instances of physical security violations at SSP and substantiated significant security deficiencies. According to the NAVINSGEN report, SSP closed most security gaps and addressed a number of deficiencies.

Based upon the findings of the NAVINSGEN report, and to ensure that SSP maintains the highest caliber of protocols and practices for the handling and safekeeping of classified information, the Secretary of the Navy has directed the Chief of Naval Operations (CNO) to confirm SSP's full implementation of the NAVINSGEN's recommendations; conduct a comprehensive security-in-depth review of SSP and, as appropriate, direct additional corrective action; provide recommendations for necessary changes to Department of the Navy policy; and, refer the final NAVINSGEN report to the relevant organizational level for considering what accountability, if any, is appropriate for individuals whom the report found to have been deficient in their performance of their duties. In addition, the Secretary of the Navy has directed the NAVINSGEN to support accountability determinations by the CNO or his designee, as may be requested.

I understand that you will provide this report to the Complainant, the President, and the House and Senate Armed Services Committees for their review. As has been the case with other reports submitted by the Department of Defense (DoD), I request that you exclude the names of witnesses in the public release of the report in accordance with the Freedom of Information Act, the Privacy Act, and DoD policy. NAVINSGEN will provide you a redacted copy of the investigation report for public release.

Again, thank you for bringing this matter to our attention. If I may be of further assistance, please let me know at your earliest convenience.

Sincerely,

Enclosure:
As stated

Ms Lewis—
I'm sorry for the long delay. I appreciate your patience
Bob

NAVAL INSPECTOR GENERAL

REPORT OF INVESTIGATION

Subj: OSC CASE DI-13-2309/2348, NAVINSGEN CASE 201303073, STRATEGIC SYSTEMS PROGRAMS

J. F. CALDWELL, JR.
VADM, USN

Edited For Public Release

Office of the Naval Inspector General
OSC Case Number DI-13-2309 & DI-13-2348
NAVINSGEN Case Number 201303073
Report of Investigation
13 August 2014

*****

Table of Contents

Table of Contents.....i
Preliminary Statement.....1
Introduction.....1
Information Leading to the OSC Tasking.....5
Summary of Findings and Conclusions.....6
Description of the Conduct of the Investigation.....9
Summary of Evidence Obtained During Investigation.....11
Allegation One.....11

What Complainants Contend..... 11
Findings..... 11
Discussion and Analysis..... 20
Conclusion..... 22
Recommended Actions..... 22
Actions Planned or Taken..... 22

Allegation Two.....23

What Complainants Contend..... 24
Findings..... 24
Discussion and Analysis..... 36
Conclusion..... 38
Recommended Actions..... 38
Actions Planned or Taken..... 39

Allegation Three.....39

What Complainants Contend..... 39
Findings..... 40
Discussion and Analysis..... 45
Conclusion..... 47
Recommended Actions..... 47
Actions Planned or Taken..... 47

Allegation Four.....48

What Complainants Contend..... 48
Findings..... 48
Discussion and Analysis..... 52
Conclusion..... 52

Recommended Actions 52
Actions Planned or Taken 52

Allegation Five.....53

What Complainants Contend 53
Findings 53
Discussion and Analysis 58
Conclusion 58
Recommended Actions 58
Actions Planned or Taken 58

Allegation Six.....59

What Complainants Contend 59
Findings 59
Discussion and Analysis 61
Conclusion 63
Recommended Actions 63
Actions Planned or Taken 63

Allegation Seven.....63

What Complainants Contend 64
Findings 64
Discussion and Analysis 66
Conclusion 67
Recommended Actions 67
Actions Planned or Taken 67

Allegation Eight.....67

What Complainants Contend 68
Findings 68
Discussion and Analysis 83
Conclusion 92
Recommended Actions 92
Actions Planned or Taken 92

APPENDIX A – FINDINGS BY ALLEGATION.....A-1
APPENDIX B – DEFINITIONS.....B-1
APPENDIX C – ACRONYMS.....C-1
APPENDIX D – INTERVIEWS CONDUCTED.....D-1
APPENDIX E - DOCUMENTS EXAMINED.....E-1

Office of the Naval Inspector General
OSC Case Number DI-13-2309 & DI-13-2348
NAVINSGEN Case Number 201303073
Report of Investigation
12 August 2014

******* Preliminary**

Statement

1. This report is issued pursuant to an Office of Special Counsel (OSC) letter to the Secretary of Defense (SECDEF), of 25 September 2013. The Office of the Secretary of Defense Executive Secretary tasked the Secretary of the Navy (SECNAV) on 30 September 2013 via Task Assign to Correspondence and Control Office to complete an investigation. SECNAV tasked the Naval Inspector General (NAVINSGEN) to conduct the investigation.

2. OSC is an independent federal agency whose primary mission is to safeguard the merit system by protecting federal employees and applicants from prohibited personnel practices. OSC also serves as a channel for federal workers to make allegations of: violations of law; gross mismanagement or waste of funds; abuse of authority; and a substantial and specific danger to the public health and safety.

3. Reports of investigation conducted pursuant to 5 U.S.C. § 1213 must include: (1) a summary of the information for which the investigation was initiated; (2) a description of the conduct of the investigation; (3) a summary of any evidence obtained from the investigation; (4) a listing of any violation or apparent violation of law, rule or regulation; and (5) a description of any action taken or planned as a result of the investigation, such as changes in agency rules, regulations or practices, the restoration of any aggrieved employee, disciplinary action against any employee, and referral of evidence of criminal violations to the Attorney General.

Introduction

4. Strategic Systems Programs (SSP) Headquarters (HQ), an Echelon II command consisting of approximately 600 civilian and military personnel, is located in Building 200, Washington Navy Yard (WNY), Washington, DC. SSP is responsible for the development, production, and life cycle support of the Navy's Fleet Ballistic Missile Strategic Weapons System. SSP reports

directly to the Chief of Naval Operations (CNO) as an Echelon II Commander, and to the Assistant Secretary of the Navy (Research, Development and Acquisition) for acquisition matters as a Direct Reporting Program Manager.[1] Additionally, SSP reports to the SECNAV as the U.S. Project Officer for the Polaris Sales Agreement with the United Kingdom (UK). Within the Department of the Navy (DON) Nuclear Weapons Enterprise, SSP is the departmental nuclear weapons technical authority, acquisition program manager and the command specifically designated to ensure DON nuclear weapons safety and security. To execute these responsibilities, SSP HQ directly oversees a distributed workforce of over 5,200 military and civilian personnel. SSP has technical oversight responsibility over all DON Ballistic Missile Submarine Fleet operations to ensure nuclear weapons safety and security, and the readiness and reliability of the Navy's TRIDENT II (D5) Strategic Weapons System. SSP has also been designated to oversee management and support for DON implementation and compliance processes with current and future international arms control agreements.

5. In 1998, under the Base Realignment and Closure Act (BRAC), SSP was moved to the Nebraska Avenue Complex (NAC), Nebraska Avenue, Washington, DC. In 2004, Congress directed the Navy, in Public Law 108-268, to relocate Navy commands and turn NAC over to the General Services Administration (GSA) for Department of Homeland Security (DHS) HQ. In 2005, SSP HQ returned temporarily to leased commercial spaces in Crystal City. Meanwhile, the Deputy Assistant Secretary of the Navy (Installations and Environment) (ASN ((I&E)) approved Special Project RM20-07 to repair, restore and modernize Building 200 to support SSP’s, as well as Navy International Programs Office (NIPO), relocation from Crystal City to a permanent facility on the WNY.

6. In April 2005, Naval Facilities Engineering Command (NAVFAC) Washington completed a master plan for Building 200, Military Construction (MILCON) Project P-402C. The plan included spaces for SSP and NIPO HQ as well as two other tenant commands. This plan addressed site improvements; construction phasing; cost estimates; and structural, antiterrorism/force protection

---

[1] SSP is identified in the Standard Navy Distribution List (SNDL) as an Echelon 2 command and the Director, SSP is considered an Echelon 2 Commander, subject to the same requirements and exercising the same organizational authority and responsibility as an officer with the title of commander, commanding officer or officer-in-charge.

(AT/FP), architectural, mechanical, electrical, and plumbing upgrades.

7. In July 2007, BAE Systems, contract support for SSP, prepared a Facility Design Criteria (FDC) for submission to NAVFAC. The FDC defined SSP requirements for spaces in Building 200 to facilitate the preparation of contract drawings and specifications for MILCON Project P-402C, Building 200, and WNY. MILCON P-402C plan for design and renovation of Building 200 was approved by W1 , Facility Acquisition and Environmental (SP20164)/SSP Project Manager/Lead on 31 July 2007. Concurrently, BAE Leads (W2 , BAE Project Lead, and W3 , BAE Project Architect) revised the FDC in October 2007 and again in January 2008, after which W1 approved SSP's FDC submission to NAVFAC. NAVFAC then published a Request for Proposal (RFP) for MILCON P-402C on 27 February 2008, ultimately awarding the contract to Forrester Construction on 30 September 2008.

8. Throughout 2009, NAVFAC continually met with stakeholders, including SSP, to refine the design plans of Building 200. NAVFAC held a security kickoff meeting with tenant commands in March 2009. Following this meeting, in April 2009, SSP submitted its SSP Security Plan to NAVFAC. The plan, prepared by BAE, included a drawing of all SSP spaces with detailed security requirements. Further, on 1 July 2009, BAE Systems Consultant provided NAVFAC with additional physical security requirements for SSP spaces. The security plan was modified on 21 July 2009, when SSP submitted additional requests for inclusion of full glass doors and/or sidelights for suite entrances. NAVFAC initially rejected this request as outside the RFP which specified the requirement for wood, but later granted the request. In August 2009, SSP also determined the need for 41 additional spaces to support additional personnel. Also in August 2009, NAVFAC's final design approval was due. During this period (2006-2010), W4 was Director, Strategic Systems Programs (DIRSSP).

9. From February 2010 through May 2010, NAVFAC addressed door hardware and architectural design criteria, as well as the fact that the doors did not have the minimum Sound Transmission Class (STC) requirements per the SSP Security Plan. In July 2010, following a meeting with NAVFAC, SSP stated on their meeting comment sheet, "Coordinate all door and hardware requirements with revised SSP Security Plans dated 14 April 2010; Door schedule does not consistently indicate STC prep; Where

possible, door additions/deletions will be verified through review of drawings."

10. In May 2010, then W5 assumed command as DIRSSP. On 29 November 2010, DIRSSP delayed the relocation to Building 200 for two weeks, because the spaces were not ready for occupancy. SSP relocated to Building 200 spaces between 17 and 20 December 2010.

11. From the occupancy of the spaces through January 2011, SSP identified multiple problems, noted on punch-lists; these included lack of window blinds, roof leaks, doors that would not close properly, telephone cabling and outlets.[2] During this period, SSP also identified problems with their Intrusion Detection System (IDS) and Access Control System (ACS); specifically the systems were malfunctioning and producing a large number of false alarms or not arming when required. Throughout this report witnesses and documents use the term Intrusion Detection System (IDS) to describe the malfunctioning alarms monitored by the WNY Dispatch Center. SSP installed separate Digital Monitoring Products (DMP) IDS for protection of secure spaces and Lenel ACS to control physical access to all SSP spaces in Building 200. The IDS provides motion sensors through the space as well as balanced magnetic switches to indicate when the doors to secure spaces are accessed. As an alarm system, IDSs are normally activated when secure work spaces are unmanned and also cover spaces that are not normally manned. The ACS represents the swipe card access through access doors. Both systems provide alarms and are monitored by the WNY Dispatch Center. Due to the large number of false alarms, Naval Support Activity, Washington (NSAW) silenced or turned off the ACS alarms. Some witness may have used IDS and ACS interchangeably.

12. SSP replaced its malfunctioning ACS with an updated ACS in November 2012.

13. Three other tenant commands are located in Building 200: the Office of the Judge Advocate General (OJAG); Naval History and Heritage Command (NHHC); and Navy International Programs Office (NIPO). Due to the missions of these other tenants, non-

---

[2] NAVINSGEN was unable to obtain the official letter of acceptance for SSP spaces in Building 200 despite several requests to NAVFAC and SSP HQ. Therefore, NAVINSGEN was unable to determine the specific date of acceptance of the spaces or the person who signed the document to accept the spaces.

Department of Defense (DoD) personnel require direct access to their offices without registry or additional screening measures. Specifically, the missions of the other Building 200 tenants are:

- OJAG's primary mission is to support the Judge Advocate General in providing legal and policy advice to the SECNAV.
- NHHC's primary mission is to maintain the official history program of the DON.
- NIPO's mission is to enable global maritime partnerships and protect critical technologies for the DON.

Note: Building 200 is not the building in which the shootings of 16 September 2013 occurred.

Information Leading to the OSC Tasking

14. The OSC tasking stems from a whistleblower complaint alleging that DON and SSP employees have engaged in conduct that may constitute a violation of law, rule, or regulation, gross mismanagement, and a substantial and specific danger to public safety.

15. OSC identified the whistleblowers as Mr. Sparky Edwards, former SSP CSM, and Mr. Vernon Londagin, former SSP Deputy CSM. The whistleblowers consented to the release of their names.

16. OSC provided the following summary of the whistleblowers' allegations:

> "The whistleblowers disclosed that between May 2012 and March 2013 they identified numerous security violations and deficiencies within the SSP Headquarters as well as other security vulnerabilities on the WNY. In brief, they alleged:
>
> Building 200, where SSP Headquarters is located on the WNY, was left unlocked and accessible to anyone on the Navy Yard on a 24-hour basis;
>
> Controlled Access Areas and Open Storage Areas within SSP spaces located in Building 200, where classified information is maintained, were not properly certified and lacked required physical security features to protect against intrusion;

> Computer systems and equipment used to receive, store, and transfer classified information were not adequately secured;
>
> Personal electronic devices were allowed in all areas of Building 200 in violation of agency regulations;
>
> Access to the WNY was granted with a showing of a driver's license, without any further inspection or proof of credentials;
>
> Concerns were reported to SSP leadership, the Office of the Naval Inspector General and Department of Defense (DoD), and other Navy and DoD components; however, the whistleblowers do not believe action has been taken to address the security violations and deficiencies reported."

17. With regard to the concerns Mr. Edwards reported to DoD IG, these matters will be handled through investigation of this OSC case (DI-13-2309/2348).

18. The tasking letter stated OSC concluded "there is a substantial likelihood that the information the whistleblowers provided to OSC discloses a violation of law, rule, or regulation, gross mismanagement and a substantial and specific danger to public safety."

Summary of Findings and Conclusions

19. This report addresses and substantiates seven of the following eight allegations:

> Allegation One: That procedures for entry to the Washington Navy Yard permitted access to people who were not properly screened, in violation of Under Secretary of Defense, Directive Type Memorandum (DTM) 09-012, Interim Policy Guidance for DOD Physical Access Control, of 8 December 2009. **Substantiated.**
>
> Allegation Two: That between May 2012 and March 2013, Strategic Systems Programs Controlled Access Areas (CAAs) and Open Storage Secret Areas (OSSs) did not meet physical and information security requirements, in violation of SECNAV M-5510.36, Department of the Navy Information Security Program, of June 2006. **Substantiated.**

Allegation Three: That between May 2012 and March 2013, Strategic Systems Programs operated a Secret Internet Protocol Router Network (SIPRNET) that was not a properly secure SIPRNET in violation of applicable Security Technical Implementation Guide (STIG) and Chief of Naval Operation/U.S. Marine Corps (CNO/USMC) Information Assurance Publication (IA-PUB) 5239-22. **Substantiated.**

Allegation Four: That between May 2012 and March 2013, the Director, Strategic Systems Programs took actions to conceal SIPRNET non-compliance from Fleet Cyber Command (FCC) Inspectors, in violation of SECNAV M-5510.36 (section 1-5), Department of the Navy Information Security Program, of June 2006. **Not substantiated.**

Allegation Five: That Strategic Systems Programs allowed Personnel Electronic Devices (PEDs) in Controlled Access Areas (CAAs) and Open Storage Secret Areas (OSSs), in violation of DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), of 14 April 2004, and SSP Instruction 8100.1, Cellular/Personal Communications System (PCS) Devices Policy at Strategic Systems Programs Headquarters, of 30 May 2008. **Substantiated.**

Allegation Six: That between May 2012 and March 2013, safes used for storing classified material in Strategic Systems Programs spaces were not properly inspected or updated with new combinations, in violation of SECNAV M-5510.36, Department of the Navy Information Security Program, of June 2006 (section 10-12).[3] **Substantiated.**

Allegation Seven: That between May 2012 and March 2013, Strategic Systems Programs personnel left Common Access Cards (CAC) unattended in workstations and positioned computer screens, displaying classified information, to face uncovered windows, in violation of DODI 1000.13; DON CIO Msg Dtd 031648Z Oct 11; and SECNAV M-5510.36, Department of the Navy Information Security Program, of June 2006. **Substantiated.**

[3] The SSP Security Manual 5510.16C, of 10 October 2003, contains the same criteria for inspecting and changing safe combinations and closely mimics most of SECNAV M-5510.36.

Allegation Eight: That between December 2010 and March 2013, the Director, Strategic Systems Programs, did not ensure all physical and information security standards were met to safeguard classified material held in the SSP spaces within Building 200 on the WNY, in violation of DODI 5200.08, Security of DoD Installations and Resources, of 10 December 2005 (as amended), SECNAV M-5239.1, Department of the Navy Information Assurance Program, of November 2005, and SECNAV M-5510.36, Department of the Navy Information Security Program, of June 2006. **Substantiated.**

20. Appendix A provides a summary of facts supporting these findings and conclusions.

21. In summary of the findings and conclusions, SSP reported to NAVINSGEN that all security deficiencies alleged by the complainants associated with SSP spaces in Building 200 have been corrected. To summarize SSP HQ:

a. Took steps to replace their ACS (completed November 2012);
b. Retracted SIPRNET cables from unsecured spaces (completed March 2013);
c. Contracted for security guards to control ingress and egress of Building 200 (completed July 2013);
d. Properly certified all spaces (completed March 2013);
e. Ordered solid core doors to replace the glass doors that were improperly located at the entry to spaces containing classified material (completed November 2013); and
f. Installed lock boxes for PEDs (completed June 2013) and upgraded their PED policy (completed November 2013).

Notes: 1) Once SSP retracted SIPRNET cables, the glass doors were no longer a security issue; however, SSP may intend to replace these doors to allow re-designation of the affected spaces. 2) SSP supported contracted security guards for Building 200 to support UK security requirements.

22. During the investigation, NAVINSGEN found no evidence to indicate loss or actual compromise of classified material.

Description of the Conduct of the Investigation

23. After receiving tasking from SECDEF, SECNAV referred the 25 September 2013 OSC tasking letter to the Office of the Naval Inspector General (NAVINSGEN) for investigation. NAVINSGEN received the tasking on 22 October 2013 and assigned case number 201303073. On 28 October 2013, NAVINSGEN assigned the SSP Inspector General (IG) to conduct an investigation. On 5 November 2013, NAVINSGEN, SSP, OJAG, NAVFAC, the Office of the General Counsel for the Department of the Navy (OGC), and Commander, Navy Installations Command (CNIC) personnel met to discuss the allegations and how the investigation would be handled. On 19 November 2013, SSP IG accepted the 28 October 2013 assignment. NAVINSGEN provided oversight in the early stages of SSP IG's investigation.

24. On 19 November 2013, NAVINSGEN contacted Mr. Edwards and Mr. Londagin, and requested interviews.[4] On 20 November 2013, Mr. Edwards and Mr. Londagin declined the interview and provided information to contact their Legal Representative. The SSP IG proceeded with the investigation; gathering documents and conducting other witness interviews. On 5 December 2013, NAVINSGEN contacted the complainants' Legal Representative, Ms. Constance Travanty, Alan Lescht & Associates, P.C., and requested assistance in scheduling an interview with her clients.

25. On 12 December 2013, Ms. Travanty notified NAVINSGEN of her clients' agreement to be interviewed. On that date, NAVINSGEN contacted Mr. Edwards and Mr. Londagin who agreed to be interviewed together on 18 December 2013. The investigation focused on allegations of security deficiencies and violations of security regulations.

26. SSP IG expanded the number of allegations due to questions from NAVINSGEN following review of preliminary reports. SSP IG submitted his last of six draft reports on 16 April 2014; however, none were accepted by NAVINSGEN. NAVINSGEN assumed the lead for the investigation from SSP IG in May 2014 due to the SSP IG's failure to show significant progress on the case. Additionally, NAVINSGEN developed additional evidence in June 2014.

---

[4] NAVINSGEN conducted complainants' interviews instead of SSP IG, due to scheduling conflicts and complainants' access to SSP spaces in Building 200.

27. During the course of this investigation 37 interviews were conducted and thousands of documents and e-mails were collected and reviewed. Attempts to conduct a key interview with the former SSP CSM, W6 (retired) were unsuccessful.

28. A Judge Advocate General Manual (JAGMAN) Investigation regarding the September 2013 WNY shooting incident inquired into the matters pertaining to allegations associated with security at the WNY.[5]

29. Security-in-depth is defined by SECNAV M-5510.36 as "a determination by the commanding officer that a command's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the command. Examples [of barriers or controls] include perimeter fences, employee and visitor access controls, use of IDSs, random guard patrols during non-working hours, closed circuit video monitoring, and other safeguards that reduce the vulnerability of unalarmed storage areas and security storage cabinets." CNO ltr Ser N09N2/10U213104 provides checklists used to certify various spaces including OSS/Secure Rooms (SR) which require security-in-depth. SSP spaces required security-in-depth due to the presence of OSSs.

30. The essence of the security-in-depth concept is that if one element of the security controls in place fails, others overlap to provide another boundary of protection for the classified information. For example, if an intruder is able to defeat the perimeter, the intruder should have to defeat another security barrier before reaching the protected information. If a command's security-in-depth plan depends on the WNY perimeter, then a problem with the perimeter makes the entry control point of a building the first line of security. Lacking any access control, such as a guard, the next layer of security would be the door to a secure area. Importantly, this is just one example of security-in-depth, and ultimately the Commander and Security Manager must define their security-in-depth plan and are required to articulate it on the OSS Checklist. Also important, US and UK security-in-depth requirements are governed by different instructions.

---

[5] A redacted copy of this report is located online at: https://www.foia.navy.mil/foia/webdoc01.nsf/(vwDocsByID)/DL140318103953/$File/WNY%20JAGMAN%20final%20report%2011mar14%20DNS36.pdf

31. WNY did not possess a secure perimeter.[6] Building 200 was an open building during the period of complaint with numerous tenants. Because the WNY perimeter was not secure and the entry doors to Building 200 were open and unguarded 24/7 this would allow a would-be intruder to approach SSP HQ on the 3rd, 4th and 5th floors. This was Mr. Edwards' concern prompting him to conduct a test of the glass and wooden framed door to SSP's CAA, demonstrating that the glass could be forced from the wooden frame with quick, concentrated physical effort. Despite this discussion, it is technically possible to meet security-in-depth requirements with a combination of other measures, which can include alarm systems, intrusion detection sensors, roving watches, cameras, etc. For clarity, security-in-depth is not required for CAAs.

Summary of Evidence Obtained During Investigation

***** Allegation**

One

That procedures for entry to the WNY permitted access to people who were not properly screened, in violation of Under Secretary of Defense, Directive Type Memorandum (DTM) 09-012, Interim Policy Guidance for DoD Physical Access Control, of 8 December 2009.

What Complainants Contend

32. The complainants alleged that access to the WNY was granted with a showing of a driver's license, without any further inspection or proof of credentials.

Findings

33. The governing law for entering military, naval, or coast guard property is found in 18 U.S.C. § 1382 and any violation of defense property security regulation is found in 50 U.S.C. § 797. The regulatory basis for physical security[7] and access control[8] on DoD installations is found in DoD Instruction (DoDI)

---

[6] Allegation 1 addresses WNY Access Control.

[7] Physical security is that part of security concerned with active and passive measures designed to prevent unauthorized access to personnel, equipment, installations, and information, and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity. It is designed for

5200.08 CH-1, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB), of 10 December 2005; and DoD 5200.08R CH-1, Physical Security Program, of 27 May 2009.

34. 18 U.S.C. § 1382 provides that "Whoever, within the jurisdiction of the United States, goes upon any military, naval, or Coast Guard reservation, post, fort, arsenal, yard, station, or installation, for any purpose prohibited by law or lawful regulation... Shall be fined under this title or imprisoned..."

35. 50 U.S.C. § 797 provides that "... a defense property security regulation is a property security regulation that, pursuant to lawful authority in (2)(A) shall be or has been promulgated or approved by the Secretary of Defense (or by a military commander designated by the Secretary of Defense or by a military officer, or a civilian officer or employee of the Department of Defense, holding a senior Department of Defense director position designated by the Secretary of Defense) for the protection or security of Department of Defense property." It further states in (3)(B) that a property security regulation is a regulation that, "otherwise [provides] for safe guarding such property against destruction, loss, or injury by accident or by enemy action, sabotage, or other subversive actions."

36. DoDI 5200.08 provides that DoD installations, property and personnel shall be protected and that applicable laws and regulations shall be enforced. It provides the authority of a DoD commander to take reasonably necessary and lawful measures to maintain law and order and to protect installation personnel and property. Chapter 3, section 3.2.2, states the DoD authority includes "the removal from, or the denial of access to, an installation or site of individuals who threaten the orderly administration of the installation or site." And Chapter 3, section 3.2.3, states the authority, "Shall not be exercised in an arbitrary, unpredictable, or discriminatory manner."

---

prevention and provides the means to counter threats when preventive measures are ignored or bypassed.

[8] A system that controls the ability of people or vehicles to enter a protected area by means of visual, manual, or electronic (or a combination of three) authentication and authorization at entry points, and manages identity information for controlling physical access to eligible, authorized persons.

37. DoDI 5200.08, Chapter 3, section 3.2.4, permits prohibiting individuals from reentering an installation after they have been removed and ordered not to reenter under 18 U.S.C. § 1382. If this order is violated, the commander of a DoD installation may detain individuals not subject to military law until the civil authorities may respond. Offenders may be appropriately prosecuted in accordance with the law.

38. DoD 5200.08R implements the policies and minimum standards for the physical security of DoD installations and resources. Chapter 3, section 3.1, states that "Access control is an integral and interoperable part of DoD installation physical security programs. Each installation commander/facility director must clearly define, consistent with DoD policy, the access control measures... required to safeguard personnel, facilities, protect capabilities, and accomplish the mission."

39. DoD 5200.08R, Chapter 3, section 3.3.1, states "Homeland Security Presidential Directive-12 (HSPD-12), mandates policy for a common identification standard for all Federal employees and contractors."

40. DoD 5200.08R, Chapter 3, section 3.3.1, further states that "The Federal Information Processing Standard 201-1 (FIPS 201-1) provides standards for the identity verification, issuance, and use of the common identity standard. The DoD Federal Personal Identity Verification credential, the Common Access Card (CAC), will provide a level of identity assurance and a method of authentication. The CAC shall be the principal identity credential for supporting interoperable access to installations, facilities, buildings, and controlled spaces. The CAC, upon presentation at perimeter security locations, shall be accepted for perimeter screening purposes."

41. DoD 5200.08R, Chapter 3, section 3.3.1.4 states, "Occasional visitors to Federal facilities will continue using a locally established, temporary issue, visitor identification system."

42. SECNAV M-5510.36, Department of the Navy Information Security Program, of June 2006, provides physical security requirements for the protection of classified information.

43. OPNAVINST 5530.14E CH-1, Navy Physical Security and Law Enforcement Programs, of 19 April 2010, implements DoD physical security and law enforcement policy, and requires installation

commanding officers to establish and maintain a Navy Security Program that implements higher headquarters requirements.

44. Commander, Navy Installations Command (CNIC) instruction, CNICINST 5530.14A, CNIC Ashore Protection Program, of 29 May 2013, implements the OPNAV physical security and law enforcement requirements for all Navy installations. The physical security and law enforcement programs safeguard personnel, property and material by enforcing rules, regulations, and law at Navy installations and activities.

45. The Under Secretary of Defense, DTM 09-012, Interim Policy Guidance for DoD Physical Access Control, establishes DoD access control policy and the minimum DoD security standards for controlling entry to DoD installations. DTM 09-012 implements the requirements of the HSPD-12 and the CNICINST 5530.14A implements DoD access control requirements and promulgates access control standards for all Navy installations.

46. WNY is the U.S. Navy's oldest shore establishment and houses the Naval Historical Center to include the Display Ship BARRY, the Navy Museum, the Navy Art Gallery, the Navy Library, and holds many ceremonial events in Leutze Park. In addition to the historical element, the official residences of CNO and other senior Flag Officers are located on the WNY, and the WNY and is home to numerous support activities for the fleet and aviation communities.

47. The DTM 09-012 states that access control standards shall include identity proofing, vetting to determine the fitness of an individual requesting and/or requiring access to installations, and issuance of local access credentials. All unescorted persons entering DoD installations must have a valid purpose to enter, have their identity proofed and vetted, and be issued, or in possession of, an authorized and valid access credential.[9] The DTM 09-012 references the DoD instruction and regulations cited above.

48. The DTM 09-012 provides that visitors to the WNY who do not possess a CAC have their identity verified and vetted at the Pass Office prior to being issued an unescorted installation

[9] Personnel who have been identity proofed and favorably vetted in accordance with the DTM 09-012 are eligible for unescorted access within the installation; but are, however, still subject to any controlled or restricted area limitations, as appropriate.

pass. Visitors must provide an authorized form of identification, e.g., driver's license. Their need for access is validated by the Pass Office that also vets visitors by using an authorized data source (The National Crime Information Center database (NCIC)) to perform a criminal background check.

49. The Judge Advocate General Manual (JAGMAN) Report of Investigation into the Fatal Shooting Incident at the Washington Navy Yard (WNY) on 16 September 2013 and Associated Security, Personnel, and Contracting Policies and Practices, 5800 N00ND of 2 November 2013, inquired into all aspects of security employed by NSAW, WNY. The JAGMAN investigation referenced local NSAW regulatory requirements established in NSAW 5560.1, Naval Support Activity Washington Traffic Policy, and NSAWINST 5532.1, Procedures for Vetting Visitors to Navy Museum on the WNY. SECDEF also directed an "internal review of the Washington Navy Yard shooting" conducted by the Under Secretary of Defense for Intelligence, dated 20 November 2013.[10]

50. The time period reviewed by the JAGMAN investigation does not correlate to the time period of the OSC allegations. However, the security concerns raised by the OSC complainants were examined in the JAGMAN investigation and concluded to be not in compliance with the methods and practices of access control at the WNY.

51. With respect to access controls at the WNY, the JAGMAN investigation concluded in Chapter 4, Finding 4.3, [redacted] Official Sensitive PSA

52. The JAGMAN investigation, Chapter 4, page 81, Fundamentals of Access Control, defined the objective of access control for entrance to installations with and without a DoD-issued CAC. Military, civilian, and contractors possessing DoD-issued CACs have their identity verified at the card issuance site and vetted according to applicable DoD personnel security standards. As such, military, civilian, and contractors possessing a CAC can properly gain access to installations via either an

[10] This review can be found at http://www.defense.gov/pubs/DoD-Internal-Review-of-the-WNY-Shooting-20-Nov-2013.pdf

electronic physical access control system or through a manned security post.

53. Visitors who do not possess a CAC, have their identity verified and vetted at the Pass Office as previously described. Visitors must provide an authorized form of identification. Their need for access is validated by Pass Office personnel, who also vet visitors by using NCIC background check.

54. As stated above, the JAGMAN investigation concluded that methods and practices employed to vet unescorted visitors at the WNY were not in compliance with local, DON and DoD instructions.

55. The JAGMAN investigation, Chapter 4, section 4.3.1 also concluded the following information. [redacted]

[redacted]

Official Sensitive PSA

[11] As defined in OPNAVINST 3501.360, DRRS-N is the Navy's capabilities-based readiness reporting system fully aligned and interoperable with the DoD DRRS. All Navy readiness reporting systems, including shore installations, shall be aligned to fulfill DRRS-N requirements... Navy commanders at all levels will have visibility on near real-time readiness data of reporting units and aggregated groups through the DRRS-N web-enabled system.

Official Sensitive PSA

[redacted]

57. W6 was the SSP CSM when SSP HQ moved into office spaces in Building 200 on the WNY. She was responsible for certifying that SSP HQ spaces in Building 200 met the physical security requirements of SECNAV M-5510.36.

58. W6 supervisor, W7 ,[12] received information in February 2011 concerning security vulnerabilities related to the WNY gate access controls. A 23 March 2011 letter from W8 , Deputy Strategic Programs Royal Navy Branch (SP50),[13] to W9 , SSP Director, Plans and Programs (SP10), references an e-mail dated 22 February 2011, wherein W7 shared WNY access control vulnerability information with W8 SP50 (UK unit) is also located in Building 200.

Official Sensitive PSA

[redacted]

60. On 25 April 2011, W10 , Management Information and Support Services Branch Head, sent a memo to W9 , via W6 and W7 , titled "SP50 Washington Navy Yard Physical Security Concerns," that addressed SP50's security-in-depth concerns. [redacted]

Official Sensitive PSA

61. On 20 July 2011, W9 sent an e-mail to W11 , Naval District Washington about the physical

---

[12] W7 retired from federal service in December 2013 and did not respond to repeated requests from NAVINSGEN for an interview.

[13] The SP50 Unit has physical security requirements for the protection of its classified material in its branch spaces as does SSP.

security and WNY access control issues. W 9 copied W 5 , W 12 , W 13 W 10 Official Sensitive PSA W 6 W 9 [redacted] akeholders to socialize a plan for security modifications.

62. As early as 20 July 2011, the DIRSSP was aware of security-in-depth and WNY access concerns based upon W 9 e-mail.

63. On 1 September 2011, W 9 again e-mailed W 11 to follow-up on his 20 July 2011 e-mail. W 9 copied W 5 , W 12 , W 13 W 10 and W 6 .

64. Mr. Edwards, SSP CSM, testified that he was appointed to his position on 29 June 2012 and shortly thereafter, used the credentials of his Deputy, Mr. Vernon Londagin, on one occasion to gain access to the WNY. He stated that Mr. Londagin was a passenger in the vehicle at the time. Mr. Edwards stated, "... So we did. I got his [Mr. Londagin's] ID one time to see how we'd get on. Well, we asked them, What if I come through because they're only checking the driver. They don't check anybody else in the car." Mr. Edwards contended that he was allowed on the WNY without an adequate identification check since the identification he presented was Mr. Londagin's. He asserted that the credentials he presented were not reviewed properly and that he used the credentials of a passenger in the vehicle while his credentials as the driver, were not properly checked.

65. Mr. Edwards testified, "What happens, they're taking – you're required – taking the card and inspecting the expiration date and ensuring it is an actual CAC card, handing it back after you make positive identification to the person that's driving, and giving it back to them. That's how they're supposed to check and they're required to check." He stated, "So how can I use that as defense in depth was my thing if I'm using his ID and they see it's me? ... People were coming in with other cards, other forms."

66. Mr. Edwards also testified that at the same time his car did not have a Naval District Washington decal. He stated, "At that time, decals were required or you're supposed to go to the visitor gate. Anybody was getting on with a driver's license." Mr. Londagin, who was interviewed at the same time, stated, "Yeah, the military personnel were pretty spot on when it came to the decal thing and checking the CAC cards or whatever. The security guards that aren't military, they don't care."

67. In a Memorandum of 18 March 2011, Assistant Secretary of the Navy (Energy, Installations and Environment), formerly ASN(I&E), eliminated the requirement for vehicles entering DON installations to be registered via vehicle decals (DD Form 2220).

68. CNO WASHINGTON DC NAVADMIN 146/13 of 29 May 2013 promulgated additional Navy policy eliminating the requirement for vehicle decals for base access, effective 1 July 2013.

69. To clarify the use of vehicle decals by NSAW between March 2011 and May 2013, NAVINSGEN NR-106 Operations Officer, W 14 was consulted as a Security Subject Matter Expert. In his civilian capacity, W 14 is the CSM for Military Sealift Command and was certified up to Security Program Integration Professional Certification through Defense Security Services in 2013. W 14 stated that prior to issuance of the NAVADMIN; decals for NSAW were required mainly for parking management. To obtain a decal, a driver had to visit the Pass Office and provide a valid license and registration as well as proof of insurance even if they possessed a CAC.

70. Aside from the complainants' testimony, we were unable to develop evidence concerning the specifics of the one particular event when Mr. Edwards used Mr. Londagin's credentials to access the WNY.

71. Mr. Edwards testified that he observed people entering the WNY unescorted at a gate using "other cards" or "other forms." He stated, "... anybody with a driver's license was coming on unchecked." Mr. Edwards provided no additional detailed information when questioned as to how he was aware what type of card was being used to gain access to the WNY.

72. We were unable to develop evidence to support or refute Mr. Edwards' allegation that people entered a WNY gate unescorted

using other cards or a driver's license. The JAGMAN investigation did conclude that the methods and practices employed to vet unescorted visitors were not in compliance with local, DON and DoD instructions. The JAGMAN investigation stated that the WNY implementation of physical security and access control policies was being further reviewed. While the JAGMAN investigation did find deficiencies in the procedures, it did not identify the use of "other cards" or "other forms" of identification as an issue of concern.

73. In his interview, Mr. Edwards alleged that when he raised his concerns regarding the leniency of WNY entry procedures, the WNY Pass Office advised that because a museum and credit union were located on the WNY, only a driver's license or state identification card was required for base entry.

74. NAVINSGEN verified through W 14 that prior to 16 September 2013, pedestrian access onto the WNY required a driver's license, state or federal identification. Visitors accessing the WNY in vehicles, presenting a driver's license, state or federal ID, with no CAC, required vetting through the Pass Office to obtain a temporary vehicle pass. The vetting for a temporary vehicle pass required a valid state license, current vehicle registration and proof of vehicle insurance and a valid purpose to enter. Vehicles could enter onto the WNY without a proper DoD decal; however, it was required that a valid driver's license, current proof of vehicle insurance and registration, or a rental car agreement that verified proof of vehicle insurance be presented.

Discussion and Analysis

75. Mr. Edwards testified that he raised his concerns of lenient entry procedures at the WNY well before the JAGMAN investigation was conducted. We find his testimony and that of Mr. Londagin credible.

76. The complainants reasonably contend that, similar to procedures at the Pentagon, general visitors to the WNY should be escorted in groups as they tour the Display Ship BARRY, the Navy Museum, and other features of the WNY. However, the DoD and DON regulations state that properly vetted visitors may have unrestricted unescorted access.

77. In 2011, SSP leadership was aware of UK security-in-depth and access concerns at the WNY, based upon W 9 e-mail

correspondences. W5 was aware of these concerns in 2011, because he was copied on W9 s e-mail and on a follow-on e-mail that requested a meeting of all WNY stakeholders. Additionally, the 25 April 2011 memo from W10 to W9 made SSP HQ leadership aware UK concerns about WNY security-in-depth vulnerabilities.

78. We find that the alleged incidents of access control leniencies that the complainants raised to OSC were possible during the time period through September 2013. We base our finding on information from W8 , the e-mails to Naval District Washington (NDW) personnel from W9 , and finally the conclusions of the JAGMAN investigation that reported deficiencies in access control methods and procedures.

79. We find Mr. Edwards' testimony credible that on one occasion he presented Mr. Londagin's credentials to the guard at a gate and was granted access to the WNY. We were unable to develop evidence about the topic aside from the complainant's testimony. We believe, however, that although not in accordance with regulations, there may have been circumstances which could have allowed it to happen. For instance, the guard could have considered that if one person in the vehicle presented credible identification, he or she represented everyone in the car. The guard could also have witnessed Mr. Londagin in the car and since the identification presented belonged to Mr. Londagin, the guard could have considered that Mr. Londagin exercised escort privileges. Regardless of the set of circumstances, without additional testimony, we believe Mr. Edwards' testimony. We believe that proper inspection and adequate identification checks were not conducted. We conclude that the access controls were, therefore, lenient and not in compliance with the DON and DoD regulations or the DTM 09-012.

80. In 2011, policies were in place to eliminate vehicle decals on Navy installations. However, W14 verified that NSAW continued to issue vehicle decals for purposes of parking management. We were unable to obtain evidence to support why the guard did not ask Mr. Edwards for identification as the driver or to address why the car did not have an installation decal. We believe that Mr. Edwards and Mr. Londagin were not directed to the Pass Office for vetting as they testified. The issuance of vehicle decal elimination may have contributed to the complainants not being directed to the Pass Office; however, without additional testimony, it is reasonable to conclude that the WNY was lenient in its access control.

81. With respect to Mr. Edwards' testimony of the use of "other cards" or "other forms" of identification such as a driver's license to access a gate at the WNY, we were unable to obtain additional evidence about the topic. We found the complainants credible and believe the methods and practices of access control for the WNY were not in compliance at the time of the alleged incident.

82. We reviewed the JAGMAN investigation and rely on its conclusions. From the information alleged by the complainants and the access control methods and practices identified in the JAGMAN investigation that concluded they did not comply with local, DON and DoD instructions and regulations; we find reason to believe the security leniencies identified by the complainants existed prior to 16 September 2013.

83. Therefore, we find that procedures for entry to the WNY permitted access to people who were not properly screened, in violation of DoDI 5200.08, DoD 5200.08R, DTM 09-012, CNICINST 5530.14A.

Conclusion

84. The allegation is **substantiated**.

Recommended Actions

85. None.

Actions Planned or Taken

86. The JAGMAN investigation identified recommendations to improve Navy capability against physical security threats.

87. In a 12 November 2013 Memorandum, SECNAV accepted the findings and recommendations of the JAGMAN investigation. The Memorandum listed 11 major findings and 14 recommendations directed to the Under Secretary, or in the absence of the Under Secretary, ASN (EI&E), Chief of Naval Operations and Commandant of the Marine Corps, Assistant Secretary of the Navy (Research, Development & Acquisition), the Deputy Under Secretary of the Navy for Plans, Policy, Oversight & Integration, and the Auditor General of the Navy for review, consideration, further investigation, and action as appropriate. SECNAV also directed that additional actions be taken to strengthen the DON

contractor requirements and to provide greater oversight on how a Sailor's or Marine's performance is evaluated and reported.

88. In an 18 March 2014 statement by the SECNAV, he reported that following 16 September 2013, "... the Navy conducted a number of rapid reviews and assessments of its bases and policies.[14] Based on these reviews [the Navy has] already made changes to improve physical security and force protection...." He also stated, "Our units have completed self-assessments to ensure their own compliance, and our Departmental leadership engaged directly with Commanding Officers around the world to stress their role in protecting our military and civilian personnel." Broader issues with the security clearance processes that involved changes to government policy were forwarded to DoD and to appropriate agencies and departments. He stated, [the Navy] worked closely with the reviews set up in the DoD, ...and with the broader government-wide review, supporting them with the information developed." Finally, SECNAV stated, "[the Navy] will implement as quickly as possible the recommendations laid out by the Secretary of Defense, including the continuous evaluation program for security clearances."[15]

89. NSAW now reports compliance with DTM 09-012 to CNIC with respect to "establishment of DoD access control policy and the minimum DoD security standards for controlling entry to DoD installations and stand-alone facilities" to implement section 1069 of Public Law 110-181.

***** Allegation**

Two

That between May 2012 and March 2013, Strategic Systems Programs Controlled Access Areas (CAAs) and Open Storage Secret Areas (OSSs) did not meet physical and information security requirements, in violation of SECNAV M-5510.36, Department of the Navy Information Security Program, of June 2006.

---

[14] This statement can be located online at: http://www.navy.mil/navydata/people/secnav/Mabus/Speech/WNYJAGMAN_Delivered.pdf

[15] DON released a list of actions completed as of 14 March 2014. This list is located on line at: http://www.defense.gov/pubs/Washington-Navy-Yard-JAGMAN_List-of-Actions_14MAR14.pdf

What Complainants Contend

90. The complainants contend that, between May 2012 and March 2013, SSP HQ had OSSs and CAAs that had a number of security deficiencies and were used without proper certification, in violation of SECNAV M-5510.36.

Findings

91. SSP HQ was previously located in the NAC Washington, DC, and then moved to Crystal City, Arlington, Virginia. By direction of the Deputy ASN(I&E), SSP relocated to the WNY, Washington, DC, in December 2010. Prior to the move, Public Law 108-268 directed NAVFAC to repair, restore and modernize Building 200, WNY, for SSP occupancy.

92. SSP HQ occupied Building 200 spaces in December 2010. W6 was the SSP CSM at that time.

93. In accordance with SECNAV M-5510.36, on 21 December 2010, W6 certified Suite SP205, Room 4200, as a SR authorized for personnel cleared to the level of information being processed; SR referred to as Open Storage Secret Area (OSS) throughout the remainder of this report.

94. On 3 March 2011, W6 certified that Suite SP202, Room 5318 was certified as OSS for classified meetings at the level of Top Secret and below in accordance with SECNAV M-5510.36.

95. On 5 August 2011, W6 certified that Rooms 4103 and 4103A were inspected and met the physical standards of SECNAV M-5510.36. She advised that they were designated as OSSs/CAAs authorized to handle and process classified materials up to the level of Top Secret.

96. SECNAV M-5510.36, Section 10-3, provides that "[c]lassified information not under the personal control or observation of an appropriately cleared person shall be guarded or stored in locked GSA-approved security container, vault, modular vault, or secure room (OSS)." In an OSS, classified information can be stored openly rather than in GSA-approved containers or vaults

when not in use. In addition, in an OSS, SIPRNET does not require a Protected Distribution System (PDS).[16]

97. SECNAV M-5510.36, Exhibit 10, provides construction standards for the approved storage areas noted above. To certify a room as OSS, SECNAV M-5510.36 includes direction pertaining to: 1) how the walls, floors, roofs, ceilings, windows, and doors are to be constructed; 2) what types of locks and hardware are required on the doors; 3) the size of utility openings; 4) access control; and 5) other security measures such as security-in-depth requirements, lock boxes, GSA-approved security containers for storage of classified information, inspections of the spaces by guards, and the use of an IDS.[17]

98. The following sections in SECNAV M-5510.36, Exhibit 10A, are relevant to this allegation pertaining to OSSs:

> 2. SECURE ROOM
>
> a. Walls, Floor, and Roof. The walls, floor, and roof construction shall be of permanent construction materials; i.e., plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other materials offering resistance to, and evidence of unauthorized entry into the area. Walls shall be extended to the true ceiling with permanent construction materials, wire mesh, or 18-gauge expanded steel screen.
>
> b. Ceiling. The ceiling shall be constructed of plaster, gypsum, wallboard material, hardwood, or any other acceptable material.
>
> c. Doors. The access door to the room shall be substantially constructed of wood, metal, or other solid material and be equipped with a built-in GSA-approved combination lock meeting Federal Specification FF-L-2740... When double doors are used, an astragal will be installed on the active leaf of the door. The hinge pins of outswing doors shall be penned, brazed, or spot welded to prevent removal. Doors other than the access door shall be secured

[16] A PDS is used to transmit unencrypted classified information through an area of lesser classification or control.

[17] Per SECNAV M-5510.36, Exhibit 10D, an IDS must detect an unauthorized or authorized penetration in the secure area. An IDS complements other physical security measures and consists of Intrusion Detection Equipment (IDE), security forces, and operating procedures.

> from the inside (for example, by a dead bolt lock, panic dead bolt lock, or rigid wood or metal bar which extends across the width of the door), or by any other means that will prevent entry from the outside. Key operated locks that can be accessed from the exterior side of the door are not authorized. Each perimeter door shall be protected by a balanced magnetic switch that meets the standards of UL 634.

99. The following sections in SECNAV M-5510.36, Exhibit 10D, are relevant to this allegation:

> 1. IDS. An IDS must detect an unauthorized or authorized penetration in the secure area. An IDS complements other physical security measures and consists of the following:
>
> a. Intrusion Detection Equipment (IDE)
> b. Security forces
> c. Operating procedures
>
> . . .
>
> 3. THREAT, VULNERABILITY, AND ACCEPTABILITY
>
> a. As determined by the commanding officer, all areas that reasonably afford access to the container, or where classified data is stored should be protected by an IDS unless continually occupied. Prior to the installation of an IDS, commanding officers shall consider the threat, vulnerabilities, in-depth security measures and shall perform a risk analysis.

100. On 7 May 2009, the CNO issued "Interim Policy Changes, Reminders, and Clarifying Guidance to SECNAV M-5510.36" mandating that OSSs be constructed per Exhibit 10A. Although CAAs, and Restricted Access Areas (RAAs) shall be designated in writing by the CSM and shall comply with the requirements in the CNO/U.S. Marine Corps (CNO/USMC) IA-PUB 5239-22 of September 2008, "IA Protected Distribution System (PDS) Publication."[18]

101. In addition, on 16 March 2010, CNO issued another "Interim Policy Change to Requirements for a Secure Room used for Open Storage Secret and Designation of Secure Rooms, Controlled Access Area and Restricted Access Area." The policy change

---

[18] CNO ltr Ser N09N2/9U223112 of 7 May 2009.

updated requirements regarding authorized supplemental controls required for an OSS and mandated the use of a template letter and updated checklists for adequate protection of classified material.[19]

102. On 29 November 2010, W15 , BAE Systems apprised W6 that the entrance to suite SP205, an OSS, would require modification with plywood panels to meet the requirements for an OSS.

103. On 14 December 2010, W15 notified W6 , via e-mail, that some of the sensors in SSP spaces in Building 200 failed to report an alarm condition when they were tested. He advised that they would retest.

104. On 13 January 2011, W6 advised NAVFAC Washington, BAE Systems, and W10 that they had been experiencing ongoing Lenel system failures since occupancy, which impacted the security of their classified assets, as well as affording access to personnel. She stated that all alarm and access control systems were offline for SSP spaces and that "we're in dire need of Convergint assistance to facilitate normal operations."

105. On 11 March 2011, W6 certified all SSP HQ spaces within Building 200 as CAAs.[20] In doing so, she certified that the physical environment[21] of SSP HQ spaces provided

---

[19] CNO ltr 5510 Ser N09N2/10U213104 of 16 March 2010.

[20] W6 also certified the spaces as a Restricted Access Area (RAA), which has the least restrictive requirements for the storage and processing of classified information. A RAA requires less security restrictions than a CAA. A RAA is a physical area (e.g., building, room, etc.) that is under physical control and to which only personnel cleared to the level of the information being processed are authorized unrestricted access. Authorized personnel are required to escort all other individuals. IA PUB-5239-22 dated September 2008, Section 2.5., P.4. RAA status is not relevant to this issue and will not be discussed further in this allegation because the complainants did not allege any deficiencies with spaces designated as RAA. Also not relevant to this allegation, but included for informational purposes only are the two least restrictive type of areas per IA PUB-5239-22: (1) Limited Access Area (LAA) - A physical area (e.g., a military base in the U.S.) that is under direct U.S. physical control and to which only authorized personnel are admitted; and (2)Uncontrolled Access Area (UAA)- A physical area (e.g., a military base in a foreign country) that is not under direct U.S. physical control and to which unauthorized personnel may gain access. Access to the area is not necessarily based upon the presentation of an approved credential. These will not be discussed further in this allegation.

[21] Physical Security Environment is defined as "That part of security concerned with physical measures designed to safeguard personnel; to prevent

adequate protection for processing classified information and met the physical security requirements of SECNAV M-5510.36.

106. A CAA has less stringent security requirements than an OSSs. Per the Information Assurance Publication (IA PUB)-5239-22, dated September 2008, Section 2.2., it is a "physical area (e.g., building, room, etc.) which is under physical control and to which only personnel cleared to the level of the information being processed are authorized unrestricted access." All other individuals are either escorted by authorized personnel or are under continued surveillance. Within a CAA, a PDS is not required for classified information processed at or below the classification level to which access to the CAA is controlled. While unprotected SIPRNET cables may run within the CAA, IA [Information Assurance] PUB-5239-22 mandates that they cannot run outside the perimeter of the CAA in a space certified at a lower standard.

107. To certify a room as a CAA, IA PUB-5239-22 includes direction to: 1) how the walls, floors, roofs, ceilings, windows, and doors are to be constructed; 2) what types of locks and hardware on the doors are required; 3) the size of utility openings; and 4) access control. It also includes other security measures such as lock boxes, GSA-approved security containers for storage of classified information, and the use of an IDS.

108. The following specific sections in IA PUB-5239-22 are relevant to this allegation pertaining to CAAs:

> 4.2. (U) Walls, Floor and Roof
>
> (FOUO) CAA: The walls, floor, and roof construction shall be of permanent construction materials (i.e., plaster, gypsum, wallboard, metal panels, hardboard, wood, plywood, or other materials) offering resistance to and evidence of unauthorized entry into the area. Walls shall be extended from true floor to true ceiling with permanent construction materials or 18-gauge expanded steel screen. If the walls cannot be extended, then an intrusion detection

---

unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage and theft." Joint Publication 1-02, DoD Dictionary of Military and Associated Terms, 8 November 2010 (As Amended Through 15 June 2014) at page 205.

system shall be installed to monitor the space above the terminal room.

4.3. (U) Doors

(FOUO) CAA: The access door to the area shall be substantially constructed of wood, metal or other solid material. The door shall be secured with a lock meeting FF-L-2890 specifications or, depending upon the security-in-depth, a lock meeting UL-437 security requirements subject to the Service [Designated Approving Authority] DAA approval. The request for waiver of a FF-L-2890 lock on the CAA door will be submitted by the command with the CTTA evaluation of the security-in-depth prepared by the Security Manager or Physical Security Officer to the Service DAA. Note: CAAs approved prior to issuance of this publication do not require the immediate installation of the FF-L-2890 lock unless the CAA is subject to remodeling or upgrade. These CAAs shall be brought to full compliance by the end of Calendar Year (CY) 10. The hinge pins of out swing doors shall be penned, brazed, or spot-welded to prevent removal. When double doors are used, an astragal will be installed on the active leaf of the door. Doors other than the access door shall be secured from the inside (i.e. by a dead bolt lock, panic dead bolt lock, or rigid wood or metal bar which extends across the width of the door), or by any other means that will prevent entry from the outside. Procedures shall be established to ensure that doors are secured at the end of the workday. During working hours the terminal area shall be: (1) occupied; (2) accessible through the use of a cipher or simplex(r) lock, or a swipe badge system; or, (3) have the doors locked when unoccupied.

4.4. (U) Windows

(FOUO) CAA: All windows which might reasonably afford visual observation of classified activities within the facility shall be made opaque or equipped with blinds, drapes, or other coverings. Windows that are less than 18 feet above the ground measured from the bottom of the window, or are easily accessible by means of objects directly beneath the windows, will be locked at all times. The locking mechanism and window construction shall be such as to provide indications

> of any attempt of forced entry. If the window construction is inadequate to provide said indication, then protective coverings, such as bars, need to be placed over the windows. The protection provided to the windows need be no stronger than the strength of the contiguous walls. Windows containing climate control units (e.g., air conditioners) must be secured in a manner to provide indications of any attempt at forced entry.

109. W6 remained the SSP CSM until she retired in December 2011.

110. In May 2012, SSP hired Mr. Edwards as the new SSP CSM. Mr. Edwards testified that, upon assuming his duties, he observed the SSP HQ spaces and reviewed the certification paperwork left behind by W6 . He conducted his own internal inspection of SSP HQ spaces to determine if they complied with security requirements contained in SECNAV M-5510.36. He also noted that W6 either used the wrong checklists or did not complete checklists when conducting her inspections. Mr. Edwards determined that SSP HQ spaces did not comply with CAA and OSS requirements set forth in SECNAV M-5510.36. He opined in his testimony that W6 falsified information in her certification of SSP HQ spaces, confirming that they met the physical security measures required by SECNAV M-5510.36 when in fact they did not.

111. On 6 June 2012, Mr. Edwards sent an e-mail to W10 , Management Information and Support Services Branch Head, advising him that although all of SSP HQ was designated as a CAA, he found deficiencies in CAAs and OSSs. He noted the following in his e-mail:

a. That the glass doors were not made of wood, metal, or some other solid material and were in violation of IA [Information Assurance] PUB-5239-22.4.3;
b. That the doors possessed clear windows, and therefore, provided views for observation in violation of IA PUB-5239-22.4.4;
c. That the IDS was not monitored in violation of IA PUB-5239-22.4.2;
d. That, because there was no building guard, the doors had to possess X09 locks or 1 inch deadbolts IA PUB-5239-22.4.3;

e. That the door hinges were not correctly installed on the inside of the doors, and therefore, were required to be pinged or welded, which was not the case, in violation of IA PUB-5239-22.4.3; and
f. That all the double doors were required to have astragals installed on them but did not, in violation of IA PUB-5239-22.4.3.

112. On 27 August 2012, SSP hired Mr. Vernon Londagin as Deputy, Physical Security Manager to assist Mr. Edwards. Mr. Londagin corroborated Mr. Edwards' testimony that SSP HQ spaces, during the time of his employment with SSP, did not comply with SECNAV M-5510.36. Mr. Londagin stated that he also noted the numerous deficiencies in the building that Mr. Edwards described when he came on board.

113. From 23 to 31 January 2013, NAVINSGEN conducted a command inspection of SSP HQ, during which the inspectors spoke to Mr. Edwards. The NAVINSGEN Command Inspection Report of SSP, dated 12 June 2013, stated that at the time of the inspection, Mr. Edwards was on board eight months and had conducted a self-assessment of SSP spaces. NAVINSGEN found that, during his self-assessment and follow-up evaluation, Mr. Edwards noted:

a. Gaps in physical and information security;
b. Lack of a functioning IDS (Mr. Edwards clearly told NAVINSGEN inspectors the SSP IDS was malfunctioning, and our report indicated the IDS malfunctioned. We were unable to confirm whether Mr. Edwards meant IDS or ACS);
c. Lack of solid core doors on spaces designated as secure areas;
d. Lack of recordkeeping on security incidents; and
e. A need to draft a new instruction and Emergency Action Plan to improve overall security awareness and practices. The NAVINSGEN report verified the deficiencies and that SSP had developed a plan of action to address these issues. This plan of action included updating instructions, emergency action plans, increasing security awareness, and proactive efforts to mitigate security shortfalls.

114. On 24 January 2013, NAVINSGEN inspectors met with SSP employees, W 10 , Mr. Edwards, Mr. Londagin, and W 16 , Special Security Representative, SSP HQ. NAVINSGEN meeting notes indicate that SSP HQ participants advised that the

alarm system for the entire WNY was outdated and grossly inadequate. Mr. Edwards stated that over 250,000 alarms went off over the 18 months, with most being phantom alarms, and because of the numerous false alarms, the alarm was currently masked. The SSP employees reported that SSP had purchased and was currently installing a new ACS for Building 200 to replace the malfunctioning ACS in place when SSP occupied Building 200.

115. W 17 , SSP Chief Information Officer (CIO), testified when Mr. Edwards first arrived in May 2012, he identified a number of interior doors within SSP HQ CAAs that were made of wooden frames, but a large portion of the center of the door was constructed of glass. Mr. Edwards advised that this construction was not in compliance with SECNAV M-5510.36. Mr. Edwards advised W 17 that he tested one of the doors by attempting to break it with a hammer. Although the glass was shatterproof and did not break, the wood strip around the side of the door broke off quickly, which did not meet security requirements. Mr. Edwards reported to W 17 that he was also concerned with the glass and the fact that it was clear. He stated this was in violation of security requirements. He noted that a bystander outside the CAA could observe a Secret safe in a CAA from outside the door. Accordingly, W 17 stated that Mr. Edwards placed white opaque coverings over the entire inside glass to make it impossible to see through and to increase the level of security.

116. W 14 testified that, after the NAVINSGEN Command Inspection of SSP, Mr. Edwards contacted him and invited him to SSP HQ to discuss SSP HQ's physical security. W 14 stated that he met with Mr. Edwards, and did a walk-through of SSP HQ spaces. He described that SSP HQ had a number of doors leading to their CAAs that were constructed of 75 percent glass in the center with a wooden frame. As these doors led to passageways and office spaces, he opined that they did not comply with IA PUB-5239-22, which required a door constructed of a solid material like wood or metal. W 14 testified that anyone without a clearance could look down the hallway and see into the CAAs.

117. W 14 also noted that in checking a designated OSS room, they were able to push up the drop ceiling. Also, they found that the wall was not a floor-to-ceiling wall as required by the security regulations. He advised that they could see over the bulkhead, making it an unsecure space. W 14 stated that he believed SSP HQ took measures to correct that

issue immediately after their walkthrough to ensure the wall was floor-to-ceiling. On 30 July 2014, W 14 confirmed by way of a walkthrough of SSP HQ's spaces that the issue had been resolved and the OSS met all security requirements.

118. W 14 corroborated W 17 testimony that he was present when Mr. Edwards and Mr. Londagin attempted to shatter the glass and that, although the glass was shatterproof, the surrounding wooden frame broke easily. W 14 testified that he discussed with Mr. Edwards the need to at least cover the glass portion with an opaque window covering to prohibit anyone from looking through the pane and make it more secure. This, W 14 surmised, was an interim measure to heighten security until the doors could be replaced.

119. W 18 , a contractor for JRC Integrated Systems, testified that during Mr. Edwards' tenure at SSP HQ the double doors on OSSs in building 200, which are required to have astragals, were deficient. She reported that this deficiency was corrected but did not relate when the correction occurred.

120. W 16 , Special Security Representative, SSP, testified, between May 2012 and March 2013, there were deficiencies with CAAs and OSSs to include the lack of a metal strip between double doors and visitor logs not being properly updated. He related that, although the visitors' identifications were checked, the logs were not adequately maintained. W 16 stated that SSP worked to correct the deficiencies but did not elaborate on what corrections were made or when they were completed.

121. Mr. Edwards and Mr. Londagin testified that in January 2013, SSP HQ leadership requested Mr. Edwards sign checklists and other documentation in preparation for an upcoming Fleet Cyber Command (FCC) Cyber Command Readiness Inspection (CCRI) certifying that SSP HQ spaces complied with security requirements. Mr. Edwards testified that he refused to sign the documents. Mr. Londagin further testified that while Mr. Edwards was out of the office he was requested to sign the documents in Mr. Edwards' absence. Both men advised that they refused to sign the documents because spaces did not comply with Navy security requirements. Mr. Londagin testified that they would not go to jail for signing documents which he knew to be incorrect.

122. On 1 March 2013, Mr. Edwards sent an e-mail to W 9 , and attached a copy of the CAA Checklist he had completed. He copied W 10 , W 19 , Deputy Director, Plans and Programs Division, and W 20 , Deputy Director, SSP, on the e-mail. In the attachment, Mr. Edwards outlined a number of deficiencies found with regard to SSP HQ physical security. The issues identified were as follows:

a. Anyone can access the base with a driver license;
b. No checks are done on those who enter the base physically or electronically;
c. Building 200 is unlocked at all times;
d. Building 200 has numerous rooms that one could hide in or conceal themselves at any time as they are unsecure at all times;
e. IDS in Building 200 does not work as it does not work more specifically in the 4200 space;
f. CCTV system is not monitored;
g. Cleared guards are not controlling or patrolling inside of Building 200 spaces;
h. Entry doors in Building 200 are not built to Physical Security requirement standards;
i. Doors do not have proper sophisticated locks installed on them;
j. Access control/deterrent hardware such as astragals is not present on doors in SSPHQ spaces;
k. No penetration testing has ever been conducted;
l. All SSP spaces are easy to penetrate undetected and exit with no evidence of penetration (Entrance can be made in less than 1 minute);
m. No threat assessment has been conducted on the building and it is an exterior barrier to the base;
n. Spaces within building 200 are easily monitored from the exterior and interior of the building;
o. Any and nearly all types of electronic devices may be found within SSPHQ spaces such as iPads, Personal Computers, WiFi cards, iPods, iPhones and etc.;
p. Access control for visitors is not adequate;
q. The fence on both sides of Building 200 is easily scaled and no guards posted for the majority of the day; and
r. No former accreditation packets were on file and spaces have been operating improperly for multiple years.

On the same date, W9 responded by e-mail, directing Mr. Edwards to see him on the next Monday to discuss the issues and walk through the document.

123. On 5 March 2013, Mr. Edwards sent an e-mail to W9 and attached a spreadsheet containing SSP HQ issues, which included the solution and the status of the action being taken for each deficiency. The list stated that no entry doors had CDX09 locks and no double doors contained astragals. In addition, he noted that the OSS and CAA packets were done incorrectly or missing. For all of these deficiencies, Mr. Edwards noted that they were being worked.

124. On 18 March 2013, Mr. Edwards sent an e-mail to W10 advising that he had informed the command that the following problems existed:

a. No adequate means to protect SIPRNET required;
b. No PDS existed for SIPRNET or lock boxes;
c. SSP HQ did not have a current designated CAA for the SIPRNET lines running throughout the command and certain areas had active network ports;
d. Room 205 was not designated an OSSs or a CAA;
e. There was no kill switch on the SIPRNET; and
f. Physical security requirements were ignored even by the head office as SIPRNET is viewed and used with windows up and left logged-on when not monitored.

In his e-mail, he opined that there should currently be no SIPRNET in the SSP HQ. He also requested notification in writing, if the command was altering security requirements; which he believed was a "large scale security violation."

125. Mr. Edwards testified that over his tenure at SSP HQ he spoke primarily with W20 and W9 regarding his security concerns. He reported that in March 2013, he asked to speak directly with W5 to put him on notice of the existing security violations. Mr. Edwards testified that, on 19 March 2013, he met with W5 to discuss his concerns regarding security. Mr. Edwards alleged he handed W5 a file and advised that he wished to discuss his security concerns. W5 testified, "I do not remember him [Mr. Edwards] handing me directly any files on potential security violation."

126. By letters dated 20 March 2013, W 10 certified that Rooms TC-42, 4103, 4103A, and 4200 in building 200 were certified and designated as secure rooms for OSS.

Discussion and Analysis

127. The complainants contend that, between May 2012 and March 2013, SSP CAAs and OSSs with a number of security deficiencies and improper certification were used in violation of SECNAV M-5510.36. We have determined by a preponderance of the evidence that, although SSP certified their spaces as being compliant with SECNAV M-5510.36, the CAAs and OSSs were not compliant and did not meet the physical and informational security requirements of SECNAV M-5510.36.

128. SECNAV M-5510.36, Department of the Navy Information Security Program, of June 2006, the Interim Policy Changes from the CNO dated 7 May 2009 and 16 March 2010, and IA PUB-5239-22 of September 2008 mandated requirements for certification of areas designated as CAAs and OSSs to ensure that classified information is properly protected. They include direction pertaining to: 1) how the walls, floors, roofs, ceilings, windows, and doors are to be constructed; 2) what types of locks and hardware on the doors are required; 3) the size of utility openings; 4) access control; and 5) other security measures such as lock boxes, GSA-approved security containers for storage of classified information, the use of guards, and the use of an IDS. The CNO also mandated checklists for CAAs and OSSs to assist the CSM in ensuring that the required and optional security measures are in place regarding their command spaces.

129. It is the CSM's responsibility to certify each room's level of security and ensure command spaces meet the security requirements of SECNAV M-5510.36. We determined that the CSM at the time SSP moved into Building 200 in December 2010 certified that the spaces met security requirements of SECNAV M-5510.36.

130. Pertaining to CAAs, the complainants alleged that despite W 6 (CSM at the time) certification of SSP spaces, the CAAs lacked solid core doors and the glass in the center of the doors allowed others to view the secured space and possibly classified information. The complainants also noted that SSP did not have a functioning ACS. These deficiencies, the complainants contend, were in violation of the above-mentioned security regulation and policies.

131. We find, by a preponderance of the evidence, that these deficiencies were present in the SSP HQ CAAs from May 2012 to March 2013. Testimony from the complainants, W 14 , and W 17 , as well as observation by the NAVINSGEN inspection team, corroborated the fact that a number of doors leading into CAAs were constructed of 75 percent clear glass with a wooden frame and not substantially constructed of wood, metal, or other solid material as required by IA PUB-5239-22.4.3. Because the SSP HQ CAA doors were not constructed of a solid material, they did not meet security requirements. We find that the IA PUB-5239-22.4.3 is ambiguous in stating what other "solid material" would be acceptable for construction of the doors. If SSP HQ CAA doors had been constructed of solid panes of shatterproof glass, they may have met the requirements of IA PUB-5239-22.4.3. However, they were not, and a test of one of the doors to withstand an intrusion proved that it could easily be compromised.

132. With regard to the glass portion of the doors, we find that the glass was not covered with an opaque covering, blinds or drapes, as required by IA PUB-5239-22.4.4 and reasonably afforded visual observation of classified activities, in violation of the IA PUB-5239.22.

133. In addition, W 10 , the complainants, and W 16 advised NAVINSGEN in January 2013 that SSP HQ did not have a functional ACS, as required by IA PUB-5239-22.4.2. They reported that SSP had ordered one and they hoped to have it functional by February 2013. We conclude this to be in violation of the IA PUB.

134. Pertaining to OSSs, the complainants alleged despite the fact that W 6 certified OSSs as compliant with security regulations, they lacked a functioning ACS and at least one OSS double door did not have an installed astragal. These are both in violation of the above-mentioned security policies.

135. We find, by a preponderance of the evidence, these deficiencies were present in the SSP HQ OSSs through March 2013. As described above, SSP lacked a functioning ACS during this period. In addition, W 18 confirmed complainants' testimony that at least one OSS's double door lacked an astragal, as required by SECNAV M-5510.36, Exhibit 10 A.2.c. The deficiency was corrected during Mr. Edwards' employment at SSP HQ.

136. Although not alleged in the complaint, W 14 also testified that, during the NAVINSGEN Command Inspection of SSP in January 2013, while conducting a walk-through of SSP spaces with Mr. Edwards, he observed an OSS with a drop ceiling that disclosed a wall within the OSS was not a floor to true ceiling wall, as required by SECNAV M-5510.36, Exhibit 10 A.2.a. and b. He noted that he popped up the drop ceiling and could see over the bulkhead, making it an unsecure space. We conclude this is a violation of SECNAV M-5510.36.

137. We conclude that, between May 2012 and March 2013, SSP HQ CAAs and OSSs did not meet physical and information security requirements in accordance with SECNAV M-5510.36. Although initially providing NAVFAC with facility requirements, to include security standards and requirements for design of SSP HQ spaces, in 2009, SSP specifically requested upgraded suite entrances with glass doors. SSP HQ accepted doors not constructed of a "solid material," as required by the IA PUB-5239-22. It was SSP's responsibility, specifically the CSM, to ensure that the facility met required security standards prior to its occupancy. We found no evidence that this was done. Instead, SSP accepted the spaces and the CSM certified that the environment provided adequate protection for processing classified information. Specifically, W 6 improperly certified that the spaces were in compliance with the physical security requirements of SECNAV M-5510.36. In fact, they were not.

Conclusion

138. The allegation is **substantiated.**

Recommended Actions

139. Should SSP require certified CAAs, they must correct any remaining deficiencies and properly certify the areas in compliance with SECNAV M-5510.36.

140. That DON clarifies SECNAV M-5510.36, Exhibit 10A, the "solid materials" that meet the security standards and, therefore, are acceptable for construction of OSS and CAA doors.

141. That SSP continue to foster a command culture conducive to security practice measures in accordance with SECNAV M-5510.36 and later policy changes.

142. That the DON consider as a best practice a team of experts approach to certifying new or renovated spaces. For large projects, certification of multiple rooms is a significant challenge requiring the review of countless details and specifications. While the security manager should ultimately be responsible and accountable, tackling this challenge would be best accomplished by employing a team of experts from NAVFAC, FCC, etc.

143. That the DON review other commands in Building 200 at the WNY to ensure their OSSs and CAAs are properly configured and certified.

Actions Planned or Taken

144. From 1 to 20 March 2013, SSP removed unprotected SIPRNET. During FCC's CCRI of SSP HQ in January 2014, FCC found SSP HQ's SIPRNET compliant with applicable standards.

145. As of 30 July 2014, NAVINSGEN, by way of a walkthrough, confirmed that the following rooms in SSP HQ have been properly certified as OSSs and are in compliance with SECNAV M-5510.36: Rooms 4103, 4103A, and SP205.

***** Allegation**

Three

That between May 2012 and March 2013, Strategic Systems Programs operated a Secret Internet Protocol Router Network (SIPRNET) that was not a properly secure SIPRNET, in violation of applicable Security Technical Implementation Guide (STIG) and Chief of Naval Operation/U.S. Marine Corps (CNO/USMC) Information Assurance Publication (IA PUB)-5239-22.

What Complainants Contend

146. The complainants contend that, between May 2012 and March 2013, SSP operated SIPRNET in SSP HQ Building 200, WNY, in CAAs and OSSs that did not meet security requirements because they were not properly certified and were lacking a PDS, lock boxes, and kill switches.

Findings

147. In addition to the findings of this allegation, the findings, analysis and conclusions of Allegation Two are adopted.

148. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), of 9 February 2011, established that the Services were required to review and implement required Security Technical Implementation Guides (STIGs), National Security Agency (NSA) security configuration guides and industry best practices to ensure DoD standard security configuration. CJCSI 6510.01F references National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 7003, of 13 December 1996, Protected Distribution System, as a source document for PDS requirements.

149. CJCSI 6211.02D, Defense Information Systems Network (DISN) Responsibilities, of 24 January 2012, requires the Services, with respect to classified data, to ensure an Authorizing Official (AO) validates all requirements to tunnel classified information across unclassified Internet Protocol (IP) infrastructure and if not, requires approval before tunneling classified data across unclassified IP infrastructure.

150. STIG CS-040, updated 5 May 2008, references the NSTISSI No. 7003, and states that classified information shall be transmitted by electronic means over an approved secure communications system authorized by the Director NSA for PDS designed and installed to meet the requirements of NSTISSI No. 7003. This STIG applies to voice, data, message (both organizational and e-mail), and facsimile transmissions. As per the STIG CS-040 and NSTISSI No. 7003, a PDS is required for any unencrypted classified data transfer, which is NOT contained within an area of classification equal to the data or higher. Secret data transfer must be protected by PDS if not within a SECRET CAA or higher.

151. CNO/USMC IA PUB-5239-22 established that while unprotected cables [SIPRNET] may run within a CAA, they may not run outside the perimeter of the CAA. If classified data is transmitted through a space of lower classification, then a PDS is required. A PDS is required when classified data traverses a hallway of lower classification from one SR to another SR, even if the hallway has some access controls at the lower level. The IA PUB 5239-22 references NSTISSI No. 7003, as a source document for PDS requirements.

152. On 11 March 2011, W6 certified that the physical environment at SSP HQ (Building 200) was mutually classified as both a CAA and RAA. As such, she certified that the environment provided adequate protection for processing classified information, including a physical and electronic constructed access control system. Specifically, W6 certified that the CAA/RAA designations were in compliance with the physical security requirements of SECNAV M-5510.36.

153. On 27 May 2011, Commander Naval Network Warfare Command issued an Interim Authorization to Operate (IATO) SSPs Classified Local Area Network (CLAN) version 4.0 on the classified legacy network. This IATO granted operation of SSP's CLAN at SSP HQ, Program Management Offices, UK Liaison Offices, and Strategic Weapons Facilities.

154. On 19 September 2011, Defense Information Systems Agency issued SSP HQ an Approval to Connect the SIPRNET, which is valid until 31 August 2014.

155. From 23 to 31 January 2013, NAVINSGEN conducted a command inspection of SSP HQ, during which the inspectors spoke to Mr. Edwards. The NAVINSGEN inspection report noted Mr. Edwards had been on board eight months and, during that time, conducted a self-assessment of SSP HQ spaces. Mr. Edwards noted shortfalls in security standards during the command self-assessment and follow-up evaluation to include: 1) gaps in physical and information security; 2) lack of a functioning intrusion monitoring system; 3) lack of solid core doors on spaces designated as secure areas; 4) lack of recordkeeping on security incidents; and 5) a need to draft a new instruction and Emergency Action Plan in order to improve overall security awareness and practices. The NAVINSGEN report verified that there were deficiencies and noted that SSP HQ developed a plan of action to address these issues, including updating instructions, emergency action plans, increased security awareness, and proactive efforts to mitigate security shortfalls. There is no information in the report concerning SIPRNET deficiencies or vulnerabilities. According to W14 Mr. Edwards raised security concerns which included SIPRNET deficiencies to the NAVINSGEN inspection team. NAVINSGEN did not report the SIPRNET deficiencies in the report, because at the time, SSP was scheduled for a March 2013 CCRI and

had an action plan that included an action to address the SIPRNET deficiencies.

156. In an 11 March 2013 e-mail, W 21 , informed W 10 and Mr. Edwards that FCC was scheduled to conduct a CCRI from 25 to 29 March 2013 to assess compliance with SSP's defense information system. However, FCC postponed this CCRI. FCC was formally rescheduled via Naval message 291940Z May 13.

157. Both the complainants and W 17 testified that in preparation for the CCRI, SSP HQ conducted an internal assessment of their compliance of cyber readiness. No timeframe for this internal assessment was identified; however, according to Mr. Edwards' e-mail of 14 March 2013, the internal assessment continued into late March 2013.

158. On 6 February 2013, Mr. Edwards e-mailed W 22 , Cybersecurity Office of the DON CIO, and provided his security concerns about the previous CSM's [W 6] certification of the CAA. As a result, he requested the definition of processing classified information, and noted that he had a problem with 220 SIPRNET ports in SSP HQ's CAA. Mr. Edwards attached a plan of action to address physical security deficiencies, specifically the glass doors.

159. On 6 February 2013, W 22 forwarded Mr. Edwards' 6 February 2013 e-mail with security concerns to W 23 , Certified TEMPEST Technical Authority, SPAWARSYSCEN Pacific, requesting that he review the information provided by Mr. Edwards and provide recommendations.

160. On 6 February 2013, W 23 notified Mr. Edwards via e-mail that if classified data lines leave the CAA or go between CAAs, then a PDS is required. He opined that based on the information Mr. Edwards provided in his 6 February 2013 e-mail that the SSP CAA did not meet the security requirements.

161. W 17 testified that the SIPRNET was not encased in a PDS because all of SSP HQ was a CCA and as a result, PDS was not required. He further testified that he advised Mr. Edwards that if Mr. Edwards decertified spaces, he would have to pull SIPRNET out of those spaces because there was no PDS. W 17 acknowledged in his testimony that once it was determined that the physical security deficiencies in the CAAs were not going to be corrected; he began pulling SIPRNET back from all of the stations outside the CAAs and OSSs. He testified that they

removed the terminals, disconnected switches, and pulled the cabling. He explained in his testimony what he meant by "pulling SIPRNET." He testified they pulled the Wyse thin client transceiver and any wires that were connected.[22] They then went into the wiring closet and through the switches, disconnected everybody from SIPRNET who were outside CAA and OSS spaces.

162. On 21 February 2013, SSP HQ notified employees via the 21 February 2013 Official Newsletter that SIPRNET terminals would be removed from SSP HQ offices, conference rooms, cubicles until SSP HQ remediates vulnerabilities in SSP HQ's CAAs. The Newsletter also stated that SIPRNET processing would be allowed in the Communications Center and room SP205. W 10 testified that SSP began removing unprotected SIPRNET on 1 March 2013 and completed the effort by 20 March 2013. In an e-mail dated 28 July 2014 to IO 1 , NAVINSGEN Investigations Branch Head, W 24 , SSP IG, corroborated that the SSP HQ IT staff began pulling back SIPRNET from unsecure spaces on 1 March 2013 and completed the pull back on 20 March 2013.

163. On 18 March 2013, Mr. Edwards sent an e-mail to W 10 , advising that he had informed the command that the following problems existed: (1) No adequate means to protect SIPRNET as required; (2) No PDS existed for SIPRNET or lock boxes; (3) SSP HQ did not have a current designated CAA for the SIPRNET lines running throughout the Command and certain areas had active network ports; (4) Room SP205 was not currently designated an OSS or a CAA; (5) there was no kill switch on the SIPRNET; and (6) physical security requirements were ignored even by SSP leadership as SIPRNET is viewed and used with windows up and left logged on when not monitored. In his e-mail, he opined that there should currently be no SIPRNET in the SSP.

164. On 18 March 2013, Mr. Edwards sent an e-mail to W 17 , asking if the SIPRNET had been turned off to all SSP HQ spaces and noted that SSP did not have "any" open storage or CAA in the SSP spaces, minus those certified for higher than secret classification. He acknowledged that the previous CSM [W 6] generated letters for CAA and OSS, but clarified that the CAA and OSS certification packets were not complete and those that she did complete, were done on the wrong form. He

[22] Wyse is a Dell "thin client" product line. A "thin client" is a low-cost, centrally-managed computer devoid of CD-ROM players, diskette drives, and expansion slots and hard drives where classified data is stored.

further stated in his e-mail that he could not certify any SSP spaces as CAAs or OSSs because the command had not yet informed him of a security-in-depth check. There is no record that Mr. Edwards decertified any CAA or OSS spaces, which as CSM would have been his responsibility.

165. On 18 March 2013, W 17 responded to Mr. Edwards' e-mail of 18 March 2013 asking if SIPRNET had been turned off. W 17 informed Mr. Edwards that he was still in the process of removing SIPRNET terminals from the SP30 space and the front office until proper physical security could be established, and further stated that SIPRNET was still operating in the Communications Center and SP205 spaces. He also informed Mr. Edwards that if he, Mr. Edwards, was directing to shut down SIPRNET in the entire command; he would have to take that to the SSP HQ Board of Directors.

166. On 14 January 2014, W 25 , SSP Deputy CIO, testified that the SIPRNET did not have PDS from May 2012 until March 2013, because the certification [CAA] by the previous CSM deemed all cabling in the "perimeter" and there was no need for those devices [PDS or lock boxes]. He further testified that due to ambiguity in physical security, they pulled the SIPRNET, with the exception of OSSs only, making the kill switch no longer a requirement. When asked what knowledge he had of SIPRNET lines being run over unsecure hallways; he confirmed he was aware questions arose about SIPRNET lines running over unsecured hallways.

167. W 10 testified that once SSP discovered that the doors and the other requirements did not meet the security requirements for a CAA, they removed the SIPRNET terminals from the offices in areas that were not OSSs. He acknowledged they removed some 200 SIPRNET terminals. He testified that they removed only so many SIPRNET cables/wiring a day and it took quite a few weeks to disconnect, inventory, and store the many terminals. According to W 10 , removal meant they disassembled and wrapped up the SIPRNET cables and disconnected SIPRNET wiring. He testified they did not shut down the entire SIPRNET but continued to maintain SIPRNET in the approved secure areas, the Communications Center and in Room SP205.

168. On 19 February 2014, W 5 testified that at the time Mr. Edwards left SSP (19 March 2013), one of the security violations that needed to be corrected was with the SIPRNET. He testified that the command made the decision to retrench/turn

off SIPRNET access to all but secure spaces until physical parameters could be put in place to properly deploy it SIPRNET to individual desktops.

169. On 16 July 2014, W 19 , testified that because they identified security related deficiencies with the glass doors in the SSP HQ spaces, they pulled the SIPRNET that was outside two certified spaces Communications Center and Room SP205. He testified that they left SIPRNET connected in the certified Secret areas.

170. Defense Information Systems Agency (DISA) conducted a CCRI of SSP from 6 to 10 January 2014. According to the CCRI Compliance Report, DISA found SSP's SIPRNET compliant with applicable directives.

Discussion and Analysis

171. The complainants contend that, between May 2012 and March 2013, SSP HQ operated a SIPRNET that was not secure because the SIPRNET existed in areas of the SSP HQ that were not properly certified as a CAA or OSS. SIPRNET requirements for a PDS and lock boxes we not met, in accordance with CJCSI 6510.01F, and applicable STIGS and CNO/USMC IA PUB-5239-22.

172. We concluded in Allegation Two that, between May 2012 and March 2013, SSP HQ CAAs and OSSs did not meet physical and information security requirements in violation of SECNAV M-5510.36. Specifically, W 6 improperly certified that the spaces were in compliance with the physical security requirements of SECNAV M-5510.36.

173. CJCSI 6510.01F and CJCSI 6211.02 establish DoD requirements for Combatant Commands and Military Services to review and implement required STIGS, and with respect to classified data, requires that classified information across unclassified IP infrastructure meets all security requirements to meet DoD standard security configuration.

174. STIGS CS-040 and IA PUB-5239-22 implements NSTISSI No. 7003 for the Navy and USMC; and requires a PDS for SIPRNET transmission outside of an area approved for unprotected transmissions.

175. NSTISSI No. 7003 requires when pull-boxes are used, they will be permanently sealed around all surface (e.g., welding

(continuous or track), compression, epoxy, fusion, etc.). If pull-boxes are used, the pull-box covers should be sealed to the pull-boxes around the mating surfaces after installation or the pull-box covers must not have removable hinge pins and must be secured with a GSA-approved changeable combination padlock. Current standards stipulate the requirements for pull-boxes for any unencrypted cabling ending in an area below CAA certification. This requirement is not germane to this allegation, due to the lack of PDS for SIPRNET within Building 200 outside OSS and certified secure spaces.

176. We found in Allegation Two that although SSP HQ spaces were certified in March 2011 as compliant with SECNAV M-5510.36, numerous physical security deficiencies were identified with the CAAs and OSSs between May 2012 and March 2013 and therefore, they CAAs and OSSs did not meet the physical and informational security requirements of SECNAV M-5510.36. Unprotected SIPRNET cabling that existed in the areas that did not comply with CAA and OSS security requirements did not meet the SIPRNET PDS and lock box security requirements of applicable STIGS and IA PUB-5239-22. As a result, we determined by a preponderance of the evidence that SSP operated a SIPRNET that was not secure and therefore, not in compliance with CJCSI 6510.01F and applicable STIGS.

177. In addition to the complainants, W 10 , W 17 and W 25 testified that a SIPRNET PDS did not exist and lock boxes and kill switches were not installed by SSP HQ, as required by applicable STIG and IA PUB-5239-22 for unprotected SIPRNET outside CAAs or OSSs. Once SSP recognized the physical security environment at SSP HQ was designated incorrectly as both a CAA and RAA, the command began removing unprotected SIPRNET that was outside the certified CAA and OSSs.

178. In addition to the complainants, W 5 , W 10 , W 25 , W 17 , and W 19 testified there were SSP HQ CAA and OSS physical security deficiencies, which resulted in the removal of the unprotected SIPRNET outside of certified secure storage areas Communications Center and SP205. SSP notified the workforce on 21 February 2013 in their official newsletter that, except for certified secure spaces (Communications Center and SP205), SIPRNET would be removed from SSP HQ offices, conference rooms, and cubicles until SSP HQ vulnerabilities were mitigated. According to testimony by W 17 and W 10 , it took SSP HQ several weeks to disconnect

SIPRNET outside the CAAs and OSSs. The effort began on 1 March 2013 and was not completed on 20 March 2013.

179. Although the complainants contend that kill switches were a requirement and the lack thereof presented a vulnerability we were unable to definitively find a codified standard requiring "kill switches" for SIPRNET lines running outside secure areas at the time in question. Having the ability to singularly shut down sections of SIPRNET via a kill switch presents stronger security. However, we were unable to validate this as a requirement. Regardless, having a "kill switch" would not remove the requirement for a PDS running outside Secret or higher CAAs.

180. We find by a preponderance of the evidence, that from May 2012 to March 2013, SIPRNET security deficiencies were present because SSP HQ had improperly certified CAAs and OSSs. As described above, SSP HQ did not have a PDS installed as required by IA PUB-5239-22 and applicable STIG for SIPR transmissions outside certified areas.

Conclusion

181. The allegation is **substantiated.**

Recommended Actions

182. SSP addressed SIPRNET issues in preparation for their CCRI in January 2014. SSP HQ was found to be in compliance in regards to their SIPRNET. There are no recommended actions.

Actions Planned or Taken

183. From 1 to 20 March 2013, SSP removed unprotected SIPRNET to spaces outside OSSs and CAAs. During DISA's CCRI of SSP HQ in January 2014, they found SSP HQ's SIPRNET compliant with applicable standards.

184. As of 30 July 2014, NAVINSGEN confirmed that the following rooms in SSP HQ have been properly certified as OSSs and are in compliance with SECNAV M-5510.36: Rooms 4103, 4103A, and SP205.

***** Allegation**

Four

That between May 2012 and March 2013, the Director, Strategic Systems Programs took actions to conceal SIPRNET non-compliance from FCC Inspectors, in violation of SECNAV M-5510.36 (section 1-5), Department of the Navy Information Security Program, of June 2006.

What Complainants Contend

185. Mr. Edwards alleged that after SSP HQ learned that the Command Cyber Readiness Inspection (CCRI) was postponed, that SSP concealed and reactivated their SIPRNET system under the same unsecured conditions.

Findings

186. In addition to the findings of this allegation, the findings, analysis and conclusions of Allegations Two and Three are adopted.

187. The complainants in their testimony stated that "while SIPRNET was shut down in some offices, SIPRNET was maintained in other offices."

188. SECNAV M-5510.36, Section 4, states "when conditions exist that prevent compliance with a specific safeguarding standard or costs of compliance exceed available resources, a command may submit a request for a waiver or exception to the requirements of this policy manual, in writing, via the chain of command to the CNO (N09N2). Each request shall include a complete description of the problem and describe the compensatory procedures, as appropriate. A waiver may be granted to provide temporary relief from a specific requirement pending completion of action which will result in compliance with this policy. An exception may be granted to accommodate a long-term or permanent inability to meet a specific requirement."

189. On 27 January 2012, W 26 , Flag Communicator, stated that he was tasked by W 17 to review SSP's security programs (Information, Industrial, Original Classification Authority, Security Education, Security Letter of Agreement, Memorandum of Agreement, Memorandum of Understanding, North Atlantic Treaty Organization Programs and Security Violations)

with members of SSP HQ security staff (W 27 , Security Specialist W 28 , W 29 , W 30 and W 31) in preparation of SSP's June 2012 CCRI.[23]

190. W 17 testimony corroborates W 26 e-mail in that he [W 17] tasked W 26 to assess SSP's physical security posture in preparation for the CCRI since he [W 26] was SSP HQ Communication Center's leading Chief and no one else had the experience.

191. On 18 June, 2012, FCC was scheduled to conduct a CCRI at SSP HQ to assess SSP HQ's compliance of their defense information system. FCC subsequently rescheduled the CCRI to October 2012 citing a schedule conflict for their command.

192. On 1 October 2012, SSP HQ was scheduled to "go-live" and transition to Navy Enterprise Resource Planning (ERP), DON's financial management system of record that standardizes Navy business practices. To eliminate operational conflicts with critical ERP transition timelines and resources and the CCRI occurring simultaneously, W 5 requested that the inspection not take place in October during the transition.

193. The CCRI was scheduled to be conducted a second time on 25 March 2013. However, due to FCC's travel restrictions, the CCRI was rescheduled for the final time for January 2014.

194. In preparation for the CCRI, SSP HQ conducted an internal assessment of their compliance with cyber readiness requirements. During their self-assessment, Mr. Edwards noted security concerns with the SIPRNET (e.g., active and unprotected lines) and contacted Defense Security Service (DSS) for assistance. Mr. Edwards assessed that the command security's posture was vulnerable.

195. Mr. Edwards contacted, via e-mail, W 32 , Physical Security Specialist, DSS, and W 33 , Chief of Security, DSS and requested that they conduct a courtesy assessment of SSP's security posture.

---

[23] W 26 served as the Flag Communicator for SSP HQ. However, an additional responsibility required that he assist the security staff with preparation for the CCRI.

196. W 32 testified that in February 2013, Mr. Edwards contacted him to assist with the upcoming CCRI as a "set of outside eyes." W 32 further testified that he conducted a courtesy assessment in early 2013 by completing a walk-around of SSP spaces. W 32 stated there was no mention of a concealed or reactivated SIPRNET during his walk-around. W 32 also testified that he did not send a report of this walk-around to SSP.

197. W 33 testified that in early 2013, Mr. Edwards contacted his physical security specialist [W 32] for assistance with SSP HQ's upcoming CCRI and asked for a courtesy walk-around with him of security concerns. Both W 32 and W 33 conducted a courtesy assessment by completing a walk-around of SSP spaces. W 33 also stated that there was no mention of a concealed or reactivated SIPRNET and that W 32 did not send SSP a report of the walk-around.

198. On January 2013, NAVINSGEN conducted a Command Inspection of SSP HQ; the inspectors found no evidence that SSP concealed or reactivated the SIPRNET.

199. On 21 February 2013, the SSP HQ staff was informed via an official newsletter that SIPRNET terminals for access to classified material would be removed from certain offices, conference rooms and individual cubicles until the physical security vulnerabilities associated with the spaces where the SIPRNET was removed were remediated. The SSP HQ newsletter informed the staff that access to SIPRNET would only be available in the Communication Center (COMCEN) and Operations, Evaluations and Training Branch (SP205) from 0700 to 1700.

200. On 11 March 2013, Mr. Edwards provided security requirements via e-mail for W 5 bi-weekly remarks to the staff in preparation for the 25 March 2013 CCRI.

201. On 12 March 2013, FCC contacted SSP and informed W 5 that the 25 March 2013 CCRI would be rescheduled for FY14. This was due to travel restrictions placed on FCC.

202. On 13 March 2013, W 34 , FCC, Original Classification Authority, e-mailed W 5 to followed-up on the verbal discussion regarding the rescheduled inspection.

203. On 14 March 2013, Mr. Edwards sent an e-mail to W 32 , and stated that "although SIPRNET access was removed from most

spaces in SSP, SIPRNET terminal access remained in W5 office and six other offices (e.g., front office staff)."

204. On 18 March 2013, W17 e-mail stated that "SIPRNET access had not been turned off in all spaces; however, the process to remove SIPRNET access was in progress. All SIPRNET terminal access was completely pulled back by 20 March 2013."

205. W17 testified that the SIPRNET terminals were removed, the switches were disconnected and the SIPR cables were "pulled back." He further testified that the SSP front office SIPRNET access was pulled back. The front office consisted of the Director, the Deputy Director, the Technical Director, and the Director Plans and Programs.

206. On 20 March 2013, SSP HQ established SIPRNET access to the designated SR. Based on W10 testimony, no changes to SIPRNET system distribution and deployment were made since 20 March 2013. Based on the information available with respect to the SIPRNET being pulled back to the secured rooms, SSP was found to be in compliance.

207. FCC postponed SSP's CCRI that was scheduled for 25 March 2013, and rescheduled the CCRI for 6 to 10 January 2014, citing FCC travel restrictions.

208. W5 testified that "the command decided to retrench the SIPRNET access to the secured spaces until proper deployment could take place."

209. W10 testified that "the SIPRNET lines were not hidden, covered up or reactivated."

210. W10 further testified that "the terminals were disconnected, inventoried and stored."

211. W19 testified that SIPRNET was "pulled back" to mitigate the unprotected SIPRNET terminals.

212. FCC conducted the CCRI from 6 to 10 January 2014; SSP received an overall grade of 88.0, one of the highest ever attained in the DON which demonstrates an external validation of SSP HQ's security operations and status.

Discussion and Analysis

213. SSP HQ experienced two rescheduled CCRI from June 2012 until January 2014 due to SSP's transition to Navy ERP and FCC's travel restrictions placed on FCC. Although the 25 March 2013 CCRI was rescheduled to FY14, SSP continued to move toward preparation for the CCRI, specifically pulling back the unprotected SIPRNET.

214. Based on testimony and documentation, and as found in Allegation Two and Three, SSP HQ identified SIPRNET security vulnerabilities. Once the vulnerabilities of the SIPRNET lines were identified, SSP pulled back the active and unprotected lines to secured spaces. The process began in February 2013 and was completed by 20 March 2013.

215. Based on testimony, SIPRNET was not concealed or reactivated once it was pulled back.

216. The NAVINSGEN Command Inspection of SSP conducted in January 2013, found no evidence of concealment. The CCRI conducted in January 2014 was assessed with a risk level indicator of low and found to be in compliance. SSP received an overall score of 88.0. The overall score of 88.0 demonstrated an external validation of SSP's security operations and status.

217. We find, by preponderance of the evidence, that the SIPRNET terminals were not concealed or reactivated under the same unsecured conditions.

Conclusion

218. The allegation is **not substantiated.**

Recommended Actions

219. None.

Actions Planned or Taken

220. None.

***** Allegation**

Five

That Strategic Systems Programs allowed Personnel Electronic Devices (PEDs) in Controlled Access Areas (CAAs) and Open Storage Secret Areas (OSSs) in violation of DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), of 14 April 2004, and SSP Instruction 8100.1, Cellular/Personal Communications System (PCS) Devices Policy at Strategic Systems Programs Headquarters, of 30 May 2008.

What Complainants Contend

221. The complainants alleged that SSP allowed PEDs in all areas of Building 200, in violation of agency regulations. The complainants explained that employees were permitted to use PEDs in CAAs and OSSs in violation of the Information Security Program requirements.

Findings

222. DoDD 8100.02 establishes a general restriction on PEDs in classified areas.

223. DoDD 8100.02, paragraph 2.3, states that this directive "Applies to all commercial wireless devices, services, and technologies, including voice and data capabilities, that operate either as part of a DOD Global Information Grid (GIG), or as part of DOD non-GIG Information Technology (IT) (stand-alone) systems. This includes, but is not limited to: commercial wireless networks and Portable Electronic Devices (PED) such as laptop computers with wireless capability, cellular/Personal Communication Systems (PCS) devices, audio/video recording devices, scanning devices, remote sensors, messaging devices, Personal Digital Assistants (PDA), and any other commercial wireless devices capable of storing, processing, or transmitting information."

224. DoDD 8100.02, paragraph 4.2, states that "Cellular/ Personal Communications Systems (PCS) and/or other Radio Frequency (RF) or Infrared (IR) wireless devices shall not be allowed into an area where classified information is discussed

or processed without written approval from the Designated Approving Authority (DAA) in consultation with the Cognizant Security Authority (CSA) Certified TEMPEST Technical Authority (CTTA)."

225. DoDD 8100.02, paragraph 4.3, states that "Wireless technologies/devices used for storing, processing, and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted unless approved by the DAA in consultation with the CSA CTTA. The responsible CTTA shall evaluate the equipment using risk management principles and determine the appropriate minimum separation distances and countermeasures."

226. SSP Instruction (SSPINST) 8100.1 prohibited cellular telephones, including photo-cable cellular telephones, in areas where classified information is discussed, processed, or electronically stored at SSP HQ during classified discussions and at all times in areas authorized for classified electronic processing. Visitors were not authorized to carry photo-capable cellular phones while in SSP spaces and were required to store them with the SSP Security Office upon check-in. The instruction did not address PEDs other than cellular telephones and had inconsistencies in application. In the opening statements, SSPINST 8100.1 specified all cellular telephones; however, throughout the remaining instruction it was specific to cellular telephones with photographic capability, and specifically the statement of compliance for all employees signature only indicated photographic capable cellular telephones.

227. SSP HQ occupied Building 200 in December 2010. On 3 March 2011, W6 , the CSM, certified Suite SP202, Room 5318 (fifth floor) as an OSS for classified meetings at the level of Top Secret and below, in accordance with SECNAV M-5510.36.

228. On 11 March 2011, W6 also certified that the physical security environment at SSP HQ was mutually classified as both a CAA and RAA. As such, she certified that the environment provided adequate protection for processing classified information, including a physical and electronic constructed access control system. Specifically, W6 certified that the CAA/RAA designations were in compliance with the physical security requirements of SECNAV M-5510.36.

229. On 5 August 2011, W 6 certified that Rooms 4103 and 4103A (fourth floor) were inspected and certified to meet the physical standards of SECNAV M-5510.36 and were designated as SRs/CAAs authorized to handle and process classified materials up to the level of Top Secret.

230. From December 2010 to November 2013, SSP permitted personnel to bring cellular telephones and other PEDs into CAAs and use them in these areas when classified information was not being discussed, processed or electronically stored in the area. An SSP employee testified on 3 June 2014 that, "Now we can't have cell phones at our spaces. They have lock boxes now in the security and in the different hallways. We lock them up now." The employee stated prior to the lock boxes being installed, "We all used our cell phones in our areas, because we had an instruction allowing us to have it." The SSP employee testified that there were some restrictions on cellular phones, "We could not have cellular phones in the Management Center (MC) during classified meetings."

231. Mr. Edwards, one of the complainants, testified that he observed a variety of PEDs, including cellular telephones, within CAAs and OSSs. He also testified that he observed SSP personnel, contractors, and visitors using cellular telephones and other PEDs in CAAs and OSSs, in violation of DoDD 8100.02.

232. W 1 , W 28 , W 17 , and W 18 , a contractor employee at SSP, confirmed through testimony that SSP personnel and others brought cellular telephones and other PEDs into CAAs and OSSs and used them in those spaces. Mr. Londagin, one of the complainants, stated SSP installed a tower or a dish on the roof of Building 200 that improved the strength of the cellular signal. Mr. Londagin stated depending on the direction the tower or dish was pointed, the signal strength improved for some wireless network providers, such as AT&T, Verizon and Sprint. At the time, DoD and SSP policy allowed PEDs in CAAs when not processing classified information.

233. Mr. Edwards testified that "intensifiers" or "repeaters"[24] were installed in OSSs around December 2012 or January 2013, to

[24] An intensifier or repeater is commonly referred to as a device to amplify a weak outside signal and bypass any obstructions to provide a strong signal to an area that was originally lacking.

improve the strength of the cellular signal, in violation of DoDD 8100.02.[25] Mr. Edwards testified, "We blocked Yahoo on the internet, so they had to get on their cell phones at their desk to check their Yahoo accounts. Instead of taking cell phones out, we intensified certain provider signals because people weren't getting good reception in their offices."

234. W 18 testified that SSP had a project to install intensifiers in rooms to intensify the cell signal. On 5 June 2014, W 18 stated that SSP personnel can no longer have cellular phones in SSP HQ spaces, but they had previously been allowed to have cellular phones, and the intensifiers provided for reception.

235. Mr. Edwards testified that in May 2012, during his initial walk-through of SSP HQ with W 10 they entered into an OSS and "there was a bookshelf inside the space and everybody's phones are in it." Mr. Edwards stated that W 10 told him, "This is where everybody puts their phones." Mr. Edwards testified, "I said, why is this in the space? This is open storage secret. It's wide open. Everybody's iPads, their personal laptops, their cameras, their phones, they're all sitting there, they're sitting there using them."

236. Mr. Edwards testified, "I requested boxes to be installed outside the door (OSS) to move them outside the area, immediately put them outside. I got that part. The rest of the space they said, draft a PED policy. I drafted it and it waited for signatures forever, they really never took action." Mr. Edwards did not provide a date for this draft, nor was the draft located. Mr. Edwards said he told them that in the interim, the devices have to be outside or they would fail the Cyber Command Inspection. Mr. Edwards testified, "DSS told them. The IG Inspector said the same thing." To address Mr. Edwards'

---

[25] Intensifiers and repeaters fall within the RF or IR devices, which are not allowed per DoDD 8100.02, paragraph 4.2, Radio Frequency (RF) or Infrared (IR) wireless devices and shall not be allowed into an area where classified information is discussed or processed without written approval from the Designated Approving Authority (DAA) in consultation with the Cognizant Security Authority (CSA) Certified TEMPEST Technical Authority (CTTA). Wireless devices are defined as technology that permits the active transfer of information involving emanation of energy between separated points without physical connection. Currently wireless technologies use IR, acoustic, RF, and optical but, as technology evolves, wireless could include other methods of transmission.

concerns there were two lock box units ordered on 4 May 2012, and they were installed in June 2012. There were additional lock boxes installed 25-26 June 2013. Prior to the lock boxes being installed, Mr. Edwards testified that there was a bookshelf inside OSS, where cell phones were stored.

237. SSPINST 5230.14, Commercial Mobile and Wireless Device, Service, and Technology Policy, of 19 November 2013, replaced SSPINST 8100.1 and established new policy and procedures for Commercial Mobile Devices (CMDs). SSPINST 5230.14 prohibits PEDs in SSP CAAs and SRs due to the increased risks of information compromise through use of new technology, but states CMDs can still be used in RAAs and Limited Access Areas (LAAs).[26] SSPINST 5230.14 also authorizes Government-owned and issued CMDs in SSP CAAs, but they must be physically removed when classified information is being electronically stored, processed, transmitted, or discussed. SSPINST 8100.1 prohibited cellular telephones, including photo-cable cellular telephones, in all areas where classified information was discussed, processed, or electronically stored; while SSPINST 5203.14 only limits prohibitions to CAA and above.

238. On 1 March 2013, Mr. Edwards reported a Security Violation (SECVIO) 03012013-008 that involved "camera phones, digital cameras and large telescopic cameras being allowed in the MC," which is a CAA, during a ceremony. The report stated the Security Manager reminded SSP leadership that cellular phones were prohibited in the MC and all visitors were instructed to leave their cameras in the Security Management office upon check-in. In passing by the MC during the ceremony, Mr. Edwards noted that approximately five cameras were visible and in plain view.

239. The SECVIO 03012013-008 report stated security measures were purposely defeated, and SSP leadership asked the CSM to perform an unethical function/practice by "turning a blind eye." Mr. Edwards provided a statement regarding the incident that read: "I received a call from W9 via my office phone during the ceremony or just shorty after it ended. W9 informed me that the command's stance on ceremonies was to turn a blind eye to this in the MC. He went on to say, I am asking you to turn a blind eye for these events."

---

[26] A physical area that is under direct U.S. physical control and to which only authorized personnel are admitted.

240. In late August 2013, W 19 was given a package of issues and allegations that Mr. Edwards provided on 19 March 2013. In a 5 September 2013 Memorandum for the Record addressing Mr. Edwards' allegation that W 9 told him to "turn a blind eye," to cameras in the MC, W 19 wrote "There was not written documentation or means to substantiate claim and essentially, it came down to being one person's word against another."

Discussion and Analysis

241. Storage and use of cellular telephones in non-classified SSP areas was not prohibited by SSPINST 8100.1 and did not violate SSP or higher guidance. However, SSPINST 8100.1 did prohibit storage and use of cellular telephones in areas when classified information was being discussed or processed. Through witness testimony it was determined that SSP personnel stored and used cellular telephones and other CMDs in CAAs and OSSs that were authorized for classified electronic processing, which was prohibited by both SSP and DOD regulations.

Conclusion

242. The allegation is **substantiated.**

Recommended Actions

243. That SSP remove any intensifying or repeating equipment that may be installed in SSP spaces.

244. That spot inspections be conducted to ensure there are no CMDs within OSSs at any time, or in CAAs when classified information is being electronically stored, processed, transmitted, or discussed.

Actions Planned or Taken

245. With the increased risk of information compromise through the use of new technology, SSP promulgated a new instruction in November 2013, SSPINST 5230.14, which established policy and procedures for the use of CMWDs. Under SSPINST 5230.14, PEDS are no longer permitted in CAAs and SRs, but PEDs are still allowed in RAAs and LAAs. SSP installed PED lock boxes in June 2013 outside of all RAAs in Building 200 for SSP personnel PED storage.

***** Allegation**

Six

That between May 2012 and March 2013, safes used for storing classified material in Strategic Systems Programs spaces were not properly inspected or updated with new combinations, in violation of SECNAV M-5510.36, Department of the Navy Information Security Program, of June 2006 (section 10-12).[27]

What Complainants Contend

246. The complainants, in their original complaint and as modified by their testimony, assert that safes containing classified information must be routinely inspected and their combinations changed 1) periodically or 2) when someone with knowledge (of the combination) leaves and no longer needs access to the safe. While they acknowledged changing combinations was their responsibility they asserted that they were unable to fulfill their duties because of "pushback" from SSP personnel who would not cooperate with them in changing the combinations.

Findings

247. SECNAV M-5510.36, Section 10-12, states that "safe combinations will be changed when first placed in use; when an individual knowing the combination no longer requires access unless other sufficient controls exist to prevent access to the lock; when subjected to compromise; or when taken out of service. Combination padlocks will be reset to the standard. Personnel who have the responsibility and possess the appropriate security clearance eligibility and access will change combinations to security containers, vaults and secure rooms." Section 7-11 of the manual states "END-OF-DAY SECURITY CHECKS Commanding officers shall establish procedures for end of the day security checks, utilizing the SF-701, Activity Security Checklist, to ensure that all areas which process classified information are properly secured. Additionally, an SF-702, Security Container Check Sheet, shall be utilized to record that classified vaults, secure rooms, strong rooms and security containers have been properly secured at the end of the day.

[27] The SSP Security Manual 5510.16C, of 10 October 2003, contains the same criteria for inspecting and changing safe combinations and closely mimics most of SECNAV M 5510.36.

The SF-701 and SF-702 forms shall also be annotated to reflect after hours, weekend and holiday activities. These forms may be destroyed 30 days after the last entry unless they are used to support an ongoing investigation required by Chapter 12.[28]

248. The allegation is most easily analyzed by dividing it into two parts; first, an examination of the "inspection" requirement and second, the requirement to change safe combinations, upon certain eventualities.

249. SSP HQ maintains roughly 186 safes certified to hold classified documents.[29] In accordance with SECNAV M-5510.36, those safes are required to be checked (inspected) daily (work days) to ensure that they are properly secured. SSP HQ personnel using the safes are responsible for conducting the end of the day review of spaces and safes. In their review they use the SF-702 to document the daily "check." The form is customarily attached to the safe. The SF-701 is used to annotate a similar required daily check of classified spaces, i.e., the SF-701 is used for rooms and the SF-702 is used for safes.

250. During the NAVINSGEN Command Inspection of SSP in January 2013, NAVINSGEN reviewed SSP compliance with the Manual's requirement for daily safe checks and found one SF-702 that was not properly completed. At that time, the complainant, who was accompanying the NAVINSGEN personnel, informed the Inspector that failure to consistently fill-out SF-702s was a continuing problem at SSP HQ; but that it was being addressed by the chain of command. Testimony collected during the SSP investigation indicated that the required checks were being performed.

251. SECNAV M-5510.36, Section 10-12, lists the necessary conditions that prompt a required combination change. Documentary evidence, in the form of e-mails, from various Codes throughout SSP, to the CSM, shows that safe combinations were being changed but the evidence was insufficient to determine the reason(s) those changes were made. When a combination is

---

[28] Per the SECNAV M 5210.1 of November 2007, the retention of the SF701/2s was reduced to one day following last entry. The one-day retention rule is the current controlling guidance; it supersedes the older 30 day retention rule.
[29] The complainants quoted several numbers in their testimony regarding the inventory of safes at SSP, their numbers ranged from around 200 to 300. The investigators were told that at the time the complainants' worked at SSP the number was 186. That number will, however, vary as particular safes are removed for maintenance.

changed it is recorded on an SF-700.[30] All SF-700s were compared against the SSP Alpha Roster.[31] Six individuals, with access to a safe, were identified as having left SSP and the combination of the corresponding safe was not changed. Those six employees all left after the period identified in the allegation.

252. W 10 testified that the complainants are responsible for changing safe combinations. Mr. Edwards is delegated this responsibility through an appointment letter designating him as the CSM. The appointment letter references the SSP Security Manual, which assigns the CSM specific responsibilities, including changing safe combinations. W 10 further testified that the complainants never reported to him that they were having difficulty in making combination changes due to resistance from individual employees or SSP leadership (as the complainants' assert in their testimony).

253. Internal SSP rules require all departing personnel to visit the Security Office for a departure clearance (CHECKOUT FORM). As a part of this process, departing personnel are required to turn in security badges and listen to a 30-minute brief. This checkout process with Security, alerts the CSM to change the combination of any safe to which the departing employee has access. The complainants, in their testimony, make it clear that they were unable to fully perform their duty to make necessary combination changes because of SSP resistance.

Discussion and Analysis

254. Documentary evidence addressing the complainant's claim that SSP HQ had a continuing compliance problem with personnel conducting the daily check and recording it on SF-702 was not found. The failure to find any documents is understandable since the regulations only require the form be kept for one day after the final entry is made on the form. Testimonial evidence concerning the daily safe inspections consisted of one person reporting they observed an incomplete SF-702. Consequently, while we did not find full compliance with the requirement for daily safe inspections the level of non-compliance was minimal. 100 percent compliance is unlikely; despite efforts to enforce

---

[30] The SF-700 is a two part form on which the combination is recorded as well as a POC named. The POC is the person who will be called if the safe is found open. Both parts contain the same information; one part is maintained in the safe and the other part in the Security Department Office.
[31] The Alpha Roster is the list of all personnel assigned to SSP.

the standard, it can reasonably be assumed that there will occasionally be an individual who forgets to fill out these forms on a given day. Significantly, there was no evidence suggesting SSP HQ personnel were ignoring this requirement or were in any way downplaying its mandatory nature. Like all activities in this area, constant vigilance is necessary to maximize compliance with the requirement.

255. While no evidence was developed establishing that one of the precipitating events occurred during the period cited in the allegation, we did determine through a review of SF-700s that, between August 2013 and January 2014, six people who had access to 19 safes left SSP HQ. Those departures, per the Manual, required SSP HQ to change the combinations of the corresponding safes or alternatively rely on other security measures being in place to keep unauthorized individuals from those safes.[32] Without a change in those combinations being made we conclude SSP HQ relied on other security measures being in place, which negated the otherwise required combination change. SSP's practice is that when an individual checks out from the command their SSP badge and access is removed. On the surface this appears to satisfy the requirement of relying on other measures to prevent unauthorized access. In hindsight there was a vulnerability with their concept because personnel could access the WNY, make their way into Building 200 and gain access through a CAA door with a glass window. Problems previously identified with access control alarms make this a security vulnerability.

256. W 10 testified that the authority and responsibility to make the combination changes belonged to the complainants. The authority and responsibility to implement the Security Program required by SECNAV M-5510.36 was delegated by DIRSSP, to the complainant as CSM. SSPINST 5510.16C, Section 8-6, places the specific responsibility of changing combinations on the CSM.

257. W 10 further testified that the complainant did not inform him that he was meeting resistance from individual employees or the SSP leadership regarding combination changes. He implies that if the complainant was experiencing problems, it was incumbent upon him to raise such concerns with his supervisor. It is clear from the facts in the other allegations addressed in this report, that the complainants did raise security concerns with SSP leadership.

[32] The Manual uses the language "other sufficient controls."

258. Failure to act in a specific matter is often shared by multiple involved individuals. The complainants' supervisor indicated that he relied on the complainants to perform their duties, including changing combinations, when needed. Reliance on subordinates to perform their duties is reasonable to a degree but it does not alleviate supervisors from providing proper oversight, to ensure those duties are being performed. After the complainants left SSP the evidence shows SSP was still not making needed combination changes. This suggests that SSP leadership both before and after the complainants left SSP were not exercising due diligence in overseeing the complainants' execution of their responsibilities and ensuring those responsibilities were being performed if the employees, for whatever reason, were not doing their duty.

259. SSP did not perform all required inspections of controlled spaces and safes.

Conclusion

260. The allegation is **substantiated.**

Recommended Actions

261. SSP conduct a review of it safes and ensure all personnel are aware of the requirements set forth in SECNAV M-5510.36 requiring combination changes. Additionally, SSP should reemphasize the need for daily inspection of secured spaces and safes.

Actions Planned or Taken

262. None.

***** Allegation**

Seven

That between May 2012 and March 2013, Strategic Systems Programs personnel left Common Access Cards (CAC) unattended in workstations and positioned computer screens, displaying classified information, to face uncovered windows, in violation of DODI 1000.13; DON CIO Msg Dtd 031648Z Oct 11; and SECNAV M-5510.36, Department of the Navy Information Security Program, of June 2006.

What Complainants Contend

263. The complainants contend that despite their repeated efforts to inform and admonish SSP HQ personnel of the requirements to safeguard their CACs and to protect computer screens from being visible to unauthorized individuals through windows, the violations continued. The complaint and the complainants' subsequent testimony reflected a level of frustration in what they perceived as SSP HQ indifference to the lapses in security, which they were repeatedly pointing out.

Findings

264. This allegation will be discussed in two parts. The first part will examine the positioning of computer screens within SSP HQ spaces, such that classified information may have been visible to individuals without appropriate clearances. The second part will address the issue of unattended CACs.

265. SECNAV M-5510.36, Exhibit 10A, states that "All windows that might reasonably afford visual observation of classified activities within the facility shall be made opaque or equipped with blinds, drapes or other coverings" and Section 7-10 states that "...classified material may not be opened or read in any area where it can be seen by unauthorized individuals."

266. The SSP FDC, MILCON Project P-402C requires blinds be provided for all SSP windows in Building 200. The NAVINSGEN Command Inspection of SSP in January of 2013 found all windows had appropriate blinds in place. The complainants' testimonial assertion appears to be that the blinds were not used, that they (the Security Department) have to constantly remind people to put the blinds down and that they met resistance from individual employees and SSP leadership in complying with their demand to lower the blinds.

267. Computer monitors are not secured to tables/desks and can be repositioned by the user. The testimony of several witnesses confirmed that there have been occasions when computer monitors were observed facing windows and had to be repositioned. Only one person testified that they specifically observed a SIPRNET computer monitor, which was on, facing a clear window.[33] The

[33] In that case, the person was told of the problem and the monitor was repositioned.

blinds, at that time, were two thirds (2/3) of the way down the window.

268. In their interview, the complainants alleged that they observed, from buildings surrounding Building 200, SSP HQ SIPRNET computers that were turned on and visible to unauthorized individuals. Mr. Edwards specifically alleged that he saw W5 SIPR monitor from across the street while standing in the parking garage.

269. W5 Flag Lieutenant (LT) was questioned over Mr. Edwards' assertion regarding the Admiral's computer monitor. The Flag LT testified that he had been in that, or similar, positions with the Admiral for 3 ½ years; throughout the time the complainants worked at SSP HQ. He provided a description of the Admiral's office and the location of the computer monitor, which was in a hutch with 1 to 2 foot sides, positioned behind the Admiral's desk, perpendicular to the windows facing the parking garage.[34] The Admiral's computer was capable of communicating on both the classified (SIPRNET) and unclassified (NIPRNET) network. A toggle switch enabled the Admiral to go from one network to the other[35]. The Flag LT testified he did not think it would be feasible for anyone to have seen the Admiral's monitor from the parking garage given the distance between them and the location of the monitor in the hutch. He also testified that he never heard of this allegation before being interviewed (25 July 2014).

270. No testimony was obtained nor was any documentary evidence found to support the complainants' general testimonial allegation that SIPRNET monitors were visible through windows from surrounding buildings.

271. DODI 1000.13, Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals. Enclosure 3. Procedures, Section 2. Guidelines and Restrictions, paragraph h: an ID card shall be in the personal custody of the individual to whom it was issued at all times. Full time possession of CACs by Navy personnel is also mandated by DON CIO Msg Dtd 031648Z Oct 11, Para 5.G.(4), which requires

---

[34] The Flag LT showed the investigator the Admiral's office and provided a description of that office, as it was configured during the complainants' tenure at SSP HQ.

[35] In February/March 2013 all SIPRNET computers throughout SSP HQ were moved to a Communication center.

all Navy personnel to "Protect Authentication tokens (E.G. Common Access Card) ... at all times ...shall not be left unattended....

272. CACs are issued to DoD personnel for personal identification purposes and for use in accessing unclassified computer systems. SSP HQ SIPRNET remote terminals do not use a CAC for logon purposes. During the time the complainants worked at SSP HQ SIPRNET computers were accessed by means of user name/passwords; after they left the command, SSP HQ transitioned to tokens in order to log onto SIPRNET.

273. Several witnesses confirmed that CACs were periodically left unattended; this was also observed during the NAVINSGEN Command Inspection of SSP. The CSM's supervisor acknowledged the problem and stated the organization was trying to correct it. If the CSM found unattended CACs, he would take them to the Security Office and the employee would have to go there to retrieve it.

Discussion and Analysis

274. The complainants suggest that monitors in general cannot face unprotected windows and that they routinely found them so positioned. SIPRNET monitors are portable and their table position can be adjusted by the user, even to the point where they are facing windows. Not surprisingly, the evidence established that monitors were moved by users and in some cases were seen facing windows. However, the various security requirements only proscribe displaying classified information, on monitors or paper copy, to unauthorized individuals. A monitor that is not displaying classified information or one that is but is in a room cloaked in closed blinds, is not in violation of any regulation. With one exception, the evidence did not establish that monitors displaying classified information were facing unprotected windows. However, that one exception is sufficient to substantiate the allegation.

275. The complainant's (Edwards) assertion, raised in his testimony, that he saw W5 SIPRNET monitor from a perch in the parking garage across the street from Building 200 is not substantiated. Based on the testimony of the Admiral's Flag LT, regarding the position and location of the monitor, the evidence does not reach a preponderance that the monitor was visible from across the street in the parking garage, let alone that the classification of any displayed information could be

discerned. There was no evidence, except as discussed above, that SIPRNET users failed to close the blinds when classified information was displayed on monitors.

276. The evidence did establish that CACs were left unintended in violation of the controlling DoD and Navy rules. Consequently, that part of the allegation is substantiated as well. It should be noted that similar to Allegation Five, the nature of this allegation likely means full compliance can never be achieved; employees will periodically forget to remove their CAC when they leave their workstation.[36] The evidence did establish that SSP was aware of the problem and was not ignoring it.

Conclusion

277. The allegation is **substantiated.**

Recommended Actions

278. That SSP continue to remind all personnel of the requirement to maintain possession of CACs at all times and to be vigilant in not exposing classified material, in any form, to unauthorized individuals.

Actions Planned or Taken

279. SSP is emphasizing employees maintain 100 percent control of CACs; the CACs which are found to be unattended are taken to security and held until retrieved by the employee with their supervisor.

***** Allegation**

Eight

That between December 2010 and March 2013, the Director, Strategic Systems Programs, did not ensure all physical and information security standards were met to safeguard classified material held in the SSP spaces within Building 200 on the WNY, in violation of DODI 5200.08, Security of DoD Installations and Resources, of 10 December 2005 (as amended),

[36] SIPRNET terminals left inactive automatically log the user off after 15 minutes.

SECNAV M-5239.1, Department of the Navy Information Assurance Program, of November 2005, and SECNAV M-5510.36, Department of the Navy Information Security Program, of June 2006.

What Complainants Contend

280. The complainants alleged that classified information under the control of the SSP HQ was not being properly protected and that it was vulnerable to compromise. The complainants specifically identified the following as security violations they believed demonstrated that SSP HQ's classified information was vulnerable:

a. Personal Electronic Devices (PED), e.g., cell phones, Wi-Fi cards, personal computers, iPads and iPods, were allowed in SSP HQ spaces where classified information was stored, processed or viewed;
b. The intrusion detection system (IDS) for SSP HQ spaces in Building 200 was defective;
c. Building 200 was an open building, left unlocked and unguarded "24/7." Anyone who gained access to the WNY was able to enter the building unchallenged;
d. Visitors and employees had access to all spaces as their command issued swipe badge IDs (provided general access into any SSP HQ space);
e. OSSs, CAAs and RAAs were never properly certified; they did not meet information security standards in accordance with SECNAV M5510.36 and IA PUB-5239.22;
f. The SIPRNET was not properly protected against intrusion and compromise; and
g. There were doors to spaces containing classified material that did not meet Navy Information Security Program standards, e.g., doors made of glass not substantially constructed from wood, metal or some solid material as per IA PUB-5239.22 and doors without proper locking mechanisms, in accordance with FF-L-2740.

Findings

281. DODI 5200.08, paragraph 3.4, state:

Commanders at all levels have the responsibility and authority to enforce appropriate security measures to

> ensure the protection of DoD property and personnel assigned, attached, or subject to their control.[37]

282. SECNAV M-5239.1, paragraph 2.4.11, states:

> Leadership support at all levels is the most important part of a command's IA program. In their role as local IA authorities Commanding Officers/Officers-in-Charge (COs/OICs) are directly responsible for identifying vulnerabilities in their operational environments and implementing the appropriate countermeasures. COs/OICs are responsible for ensuring that personnel under their command are trained and abide by IA policy. Commanders of DON organizations shall ensure that all IT assets they oversee and operate are accredited and operated in accordance with the accreditation documentation.

283. SECNAV M-5510.36 requires DON commanding officers to manage their command's Information Security Program (ISP) in compliance with that manual. The manual specifies what safeguards are required for classified material handling and storage. Regarding the basic requirement for the proper storage of classified materials, the manual specifically states in Chapter 10 that:

> Commanding officers shall ensure that all classified information is stored in a manner that will deter or detect access by unauthorized persons. Classified information that is not being used or that is not under the personal observation of cleared persons who are authorized access shall be stored per this chapter. To the extent possible, limit areas in which classified information is stored and reduce current holdings to the minimum required for mission accomplishment.

284. In May 2010, then W5 assumed command as DIRSSP.

285. As previously noted, Mr. Edwards was the SSP CSM from May 2012 to March 2013. He was preceded in that position by W6 . She left her position with SSP and retired

---

[37] DODI 5200.08 was changed on 19 May 2010 (CH-1) and again on 8 April 2014 (CH-2). The requirement for commanders at all levels to "enforce appropriate security measures" was not changed.

from Federal service in December 2011, approximately six months before Mr. Edwards was hired.[38]

286. There was inconclusive testimony about who may have been the "acting" CSM during the period of time between W 6 retirement in December 2011 and the hiring of Mr. Edwards in May 2012. W 10 testified that he believed that it was "probably" W 7 , who was at the time the Branch Head over W 6 and W 10 . W 10 testified that W 7 may have performed the duties of the CSM, however, he stated that he did not "really know if there was ever an official letter designating anybody during that time."[39]

287. W 6 was the SSP CSM when SSP occupied office spaces located in Crystal City and during the time that Building 200 was being remodeled. As the CSM, she was responsible for certifying and accepting SSP spaces for compliance with physical security and information security requirements.

288. SSP HQ relocated from Crystal City to Building 200 on the WNY in December 2010. After SSP HQ relocated to Building 200, W 6 identified problems with the operation of the ACS that was installed during the renovation project. On 13 January 2011, she reported the problems she had become aware of to W 35 , a NAVFAC employee, who served as the Building 200 Construction Project Manager and oversaw the building's renovations from 2008 to 2010. W 6 wrote in an e-mail to W 35 on 13 January 2011 that all alarm and access control systems were off-line for the SSP HQ spaces on the second and fourth floors in Building 200.

289. W 10 testified at length about the faulty ACS that had been installed in Building 200, before occupancy, and the trouble that SSP HQ experienced with the alarm system in the months following SSP HQ's move into Building 200. W 10 stated:

---

[38] Mr. Edwards accepted a career-conditional appointment as a supervisory security specialist at SSP effective 20 May 2012. He was designated in writing as the SSP Security Manager on 29 June 2012.

[39] W 6 was not interviewed. Although she acknowledged receipt of our certified mail letter requesting that she be interviewed, W 6 did not respond to our subsequent attempts to speak with her on the phone.

> We started finding as we moved in here that we were getting alarms showing up and we have a monitoring system here that we would monitor and you'd see alarms coming up [and the system would identify the alarm source] it's this door, let's say, and we would go check and that door's really not -- there's nothing wrong with it. It's not unlocked. It's not open. The base also monitors that and the base was sending over the policemen and, you know, the security guards all the time to -- check them out. So we got -- we contacted the installer, the people who installed the security system. It's a Lenel [ACS] security system. It's the same one the majority -- a lot of -- a number of the organizations on the base use. So it all ties into the same system.
>
> We met with NAVFAC. We met with Naval Support Activity Washington folks who monitor the alarm systems, [and tried] to get them to figure out why this was happening. We got with the -- Convergent, which was the company who installed it, and they were a subcontractor to the building renovation effort, to try and figure what was going on. The base started -- I believe they were -- they started masking the alarms during working hours.
>
> . . .
>
> We would still get them every day. We would get them and we would go through them and check them out. So we weren't ignoring them at all. It was the base during working hours. Now, they would not ignore any of our secure areas, the open storage areas. [If an] alarm came over, they were over here in a minute. If it was an [alarm for a sensor] they hadn't seen before, they would call us.

290. Despite the malfunctioning ACS, on 11 March 2011, Ms. Bryant-Gordon certified that the spaces SSP HQ occupied in Building 200 met physical security requirements of SECNAV M-5510.36. She also specifically certified that SSP HQ spaces were mutually classified as both a CAA and RAA. As such, she erroneously certified that SSP HQ spaces provided adequate protection for processing classified information and that appropriate access controls were in place. Based on other discrepancies with physical security identified throughout the

report, her certification of CAA spaces was defective from the start.

291. Around the same time that W6 made her certification, W7 , W6 supervisor, received information that the access control procedures at the WNY were lacking. Although we were unable to obtain a copy of W7 22 February 2011 e-mail, we know she shared this security vulnerability information with SSP HQ staff, to include the Strategic Programs Royal Navy Branch (SP50). The SP50 offices were located in Building 200.

292. On 23 March 2011, W8 sent a letter to W9 ssing concern about the security vulnerability information W7 had reported in her 22 February 2011 e-mail about WNY gate access control procedures. In his letter to W9 , W8 wrote:

Official Sensitive PSA

[redacted]

Official Sensitive PSA

[redacted]

293. W8 requested W9 inform him what steps would be taken to bring the level of security at Building 200 up to the standards that were in place when SSP HQ occupied office spaces in Crystal City. In response to W8 s request, W9 directed a meeting for concerned parties, which was held on 5 April 2011 and attended by SP50 and SSP Security Department personnel. During the meeting, SP50 explained the process required for developing their (UK) security rating posture and what was necessary to achieve an acceptable security rating. Thereafter, on 25 April 2011, a summary of the meeting and the SP50 security requirements were reported back to W9 .

294. On 20 July 2011, W9 e-mailed W11 Naval District Washington about the physical security and WNY access control issues that had been reported to him. W9 copied W5 , W12 W13 W10 and W6 on his e-mail and wrote:

Official Sensitive PSA

[redacted]

Official Sensitive PSA

[redacted]

295. The foregoing finding can affect the security situation in Building 200 for all tenant commands with classified information holdings in their respective Building 200 office spaces, not just the UK contingent. For example, proper protection of classified information for certain spaces (OSSs) relied upon a layered defense as described in SECNAV M-5510.36. In this case, the WNY base entry access control points had been assessed to be inadequate to prevent unauthorized entry into Building 200. At the time and until June 2013, Building 200 did not have guards or any other measures to control entry into the building. It was reasonable to believe, therefore, that anyone gaining access to the WNY could also enter Building 200 undeterred and attempt to gain entry at the door to any of the spaces containing classified information located in the building. Based on W 9 e-mail, this situation did not meet UK information security standards for the protection of classified information.

296. On 1 September 2011, W 9 e-mailed W 11 again to follow-up on his 20 July 2011 e-mail that requested a meeting with the NDW Director of Security, W 36 , and appropriate other NDW and WNY officials to discuss the ongoing security shortfalls identified about access to the WNY and in particular Building 200. W 9 repeated his prior request for "a meeting with all WNY stakeholders" to review SSP's planned changes to security procedures at Building 200. He copied W 5 , W 12 , W 13 , W 10 and W 6 on his e-mail.

297. Throughout the intervening months, W 9 and W 10 continued to engage with officials at NDW and NAVFAC Washington to arrange for security guards at Building 200. Their efforts eventually resulted in a contract being awarded for security guards to control access into Building 200. However, security guards were not in place until June 2013 and procedures for 100 percent ID check of anyone seeking access to Building 200 were not established until September 2013. The delay in achieving 100 percent ID check was because SSP as one of several tenants in Building 200 had to coordinate with the other tenants about the procedures they planned to put into place. W 24 , SSP IG, explained as follows:

> During the initial phasing in of the guard services in June 2013 it was decided to gradually acclimate SSP and the tenants of Bldg 200 to the new guard force requirement. In July 2013 NAVFAC (W 37 , COTR) asked SSP to provide Post Orders and modify the Scope of Work for the new guard services. Post Orders had to be developed in concert with the other tenants of Bldg 200, by acknowledging and incorporating the different requirements of their specific missions. Some of the topics that had to be worked out were hours of operation, visitors, tenants POC's, authorized ID cards, and access doors to name a few. Once all the factors of the Scope of Work and Post Orders were worked out with SSP, NAVFAC and the tenants the 100% ID check was implemented for Bldg 200 in September 2013.

298. Mr. Edwards testified that he personally identified the same vulnerabilities about the WNY access control checkpoints after he took over as SSP CSM; the vulnerabilities that W 7 identified and reported to SSP HQ staff on 22 February 2011. In addition to notifying W 9 about his own security vulnerability assessment of inadequate access control onto the WNY, Mr. Edwards testified that he also notified the WNY Visitor Control Center, the WNY Police, and WNY Commanding Officer, W 38 .[40]

299. Based on the documentary evidence we reviewed and Mr. Edwards' testimony, it was clear that Mr. Edwards began identifying security problems and reporting them to his chain of command starting in June 2012. As an example, on 6 June 2012, Mr. Edwards sent an e-mail to W 10 , copied W 7 and several others and stated:

> I want to address a couple [of] things that came from my meeting earlier. The SSP has all of its spaces at the CAA standing. The problem with this is that there is a massive shortfall in some major areas.

---

[40] On 6 December 2013, W 38 , Commanding Officer, Naval Support Activity, Washington, testified that he had no knowledge that Mr. Edwards conducted an independent assessment of base access controls or antiterrorism/force protection procedures at the WNY. Also, NAVINSGEN did not identify anyone at the WNY Visitor Control Center or WNY Police with knowledge of these events.

300. Mr. Edwards continued his e-mail listing the various shortfalls that he had noted and listed:

a. Glass doors not meeting the IA Pub 5239-22.4.2 standard;
b. Clear vice opaque windows in spaces that contained or where classified information was viewed;
c. IDS not monitored;
d. X09 door locks were not installed as required for a building that was unguarded;
e. Improper door hinges; and
f. Double doors missing astragals.

301. On 16 October 2012, W9 emailed Mr. Edwards about the command security news letter Mr. Edwards prepared and forwarded to W9 for his consideration and comment. The proposed newsletter for SSP staff spoke to ongoing efforts by the CSM to increase security conditions in Building 200. In his email reply to Mr. Edwards, W9 wrote:

> I have made a few edits to your Security Newsletter (see 1st attachment shows track changes, 2nd attachment is clean version). Please review to make sure I did not change the context of your letter and if you are OK with the changes, W20 will issue as an all hands email with the text from the clean version.
>
> Also note that I added "core" hours. Since the base opens the main gates at 0530, people begin the normal day at that time, so I made that the start date. I thought 1800 in the evening was reasonable. So people will need to scan in the front door between 1801 in the evening and 0529 in the morning. I think that is fair. Please confirm that the message is OK so that we can send out. Thanks
>
> Also this is a good way to get the message out. We have buy-in from the BOD and SPOO as W19 and I pre-socialized this message. So we are all behind the improvements you are making. Again I just want to stress it all about how we deliver the message which make a huge difference on how the message is received.

302. On 20 October 2012, Mr. Edwards emailed several SSP officials about security violations that he noted they were

responsible for. Mr. Edwards explained in his email to these individuals that they had not properly protected For Official Use Only, Personally Identifiable Information, Unclassified Controlled Nuclear Information and/or Restricted SSP documents as required by the command security instruction. W9 was copied on Mr. Edwards' 20 October email and in reply to it, on 22 October 2012, W9 wrote to Mr. Edwards and W10 and copied the W20 stating:

> Sparky/Bill,
>
> While everything that you are doing regarding security is the "right thing" to be doing, I again want to emphasis that it is all about message delivery where people perceive that they were unaware of the rules (because they were overlooked for so long) and feel blind-sided. So when delivered in a "gotch-ya" environment it is not received as well as when we roll out "expectations" first, then come behind with recommended improvements by doing test walk around with the Branch deputy and Branch Security officers. Then after all understand expectation, we can purposely call them out for violations.
>
> So here is the plan, I am directing that you develop a security all hands presentation to be rolled out at the next senior leadership so we can get feedback and a feel for how it will be perceived. Then refine it to be rolled out to all hands. The presentation should include what we believe are best practice expectations, what should your work space look like when you depart for the day. How should material be protected, covered, etc? What should the branch security officers be looking for and how should branch security duty be performed? What are the responsibilities of the branch security officer of the day when he signs off that a space is free and clear of classified or protected material?
>
> Bottom line is we need to make sure they understand the rules first, then we can begin to enforce them.

303. NAVINSGEN inspected SSP from 23 to 31 January 2013 as part of NAVINSGEN's periodic requirement to inspect all U.S. Navy Echelon II commands. During this inspection, the NAVINSGEN team noted that the Security Manager, Mr. Edwards, had compiled a

comprehensive list of security deficiencies and proposed corrective actions. Commenting in the executive summary of the 12 June 2013 SSP command inspection report, the Inspector General stated in the Administrative Program Compliance and Oversight section of the summary that NAVINSGEN inspectors found the SSP security program missing key elements and not compliant with governing instructions. Specifically, the summary stated:

> The SSP Command Security program instruction and the Emergency Action Plan are not current or in accordance with DON regulations. Many aspects of the signed security instruction do not apply to SSP's current facilities. SSP has progressed with resolving many of the security concerns revealed during SSP's self-assessment. The command security instruction and Emergency Action Plan are in draft form, being revised to comply with current security directives. NAVINSGEN recognized SSP's ability to self-assess and proactively take steps to improve security practices. A current, revised command security program instruction will solidify the security foundation to ensure the command adheres to the governing security policies, instructions, and directives.

304. In preparation for an expected, but later postponed, CCRI, SSP HQ went about addressing discrepancies. For example, on 21 February 2013, page 1 of the SSP command newsletter included the following announcement related to SSP HQ's ongoing efforts to correct its SIPRNET discrepancies:[41]

> SPHQ SIPRNET Operations
>
> Several changes are being made to increase the security of SSP networks:
>
> Commencing 1 March - With the exception of the COMCEN (Room 4103) and SP205 (Room 4200), SIPRNET terminals will be removed from SPI IQ offices, Conference Rooms, and cubicles until SPHQ remediates CAT I vulnerabilities in SSP's Controlled Access Area (CAA). In the interim, SIPRNET processing will only be

[41] From 6 to 10 January 2014, SSP underwent the Command Cyber Readiness Inspection. SSP received a grade of "Excellent" and a score of "88%." All areas were assessed as "compliant" and SSP's level risk indicator was determined to be "low."

> allowed in the COMCEN and SP205 from 0700-1700. For Emergency (Infrequent) access to the COMCEN outside of these hours, please contact the SPHQ Command Duty Officer (CDO) at (571) 481-7438. For Emergency (Infrequent) access to SP205 outside of these hours, please contact the SP205 Duty Officer (DO) at (571) 481-7446.
>
> For Branches that require FREQUENT access to the COMCEN or SP205 outside of these hours, have the Branch Head contact and provide W 26 with a list of the required personnel via the MIS [Management Information System] Help Desk at (202) 433-8777.

305. On 1 March 2013, Mr. Edwards wrote an email to W 9 and requested that Mr. Kethcum review a draft security-in-depth (SID) determination document Mr. Edwards prepared for W 20 signature. The document requested W 5 determination of SID in order to designate certain SSP assigned space in Building 200 as an OSS.

306. During their clarification interview, the complainants testified and provided additional information about the security concerns they reported up their SSP chain of command; the same concerns they raised in their complaint to the OSC. In particular, the complainants stated they reported that Building 200 was vulnerable because there were insufficient measures to prevent unauthorized access. The complainants noted in particular that the concept of security-in-depth was specifically lacking for the SSP HQ spaces located in Building 200. Both complainants testified that they reported their concerns about security-in-depth to W 9 [42]

307. During the time in question, NDW granted access onto the WNY to anyone with a valid State or Federal ID. Also during this time, Building 200 did not have security guards posted; consequently, anyone who gained access to the WNY could enter

---

[42] Based on our review of the evidence, security-in-depth as defined by the SECNAV M-5510.36 was never defined for OSS spaces as required by CNO Policy Memo of 16 MAR 2010. According to Mr. Edwards, as CSM, he attempted to work with his leadership to establish a security-in-depth plan. Mr. Edwards' testimony suggests that in his professional opinion and as evidenced throughout this report, SSP lacked adequate security to satisfy security-in-depth requirements.

the building's common areas 24/7 without being challenged or their purpose for entering Building 200 determined.[43]

308. W9 was interviewed on 16 January 2014 and he testified about his knowledge of the physical and information security concerns that Mr. Edwards reported to him. About those reports, W9 said:

> Mr. Edwards and I had a conversation regarding deficiencies he found during his reviews. I formally asked that he provide a list [from which SSP could take] corrective actions to bring our security standards in alignment with what he thought were the standards at the time.
>
> . . .
>
> [Mr. Edwards] stated these were requirements but no documents were provided. You can say that something was wrong but you have to show the requirements so I can understand it because I was trying to distinguish between [Mr. Edwards' expectation] and a requirement. Finally, no, he did not bring any violations to my attention.

309. Although Mr. Edwards testified that he had regular communication and meetings with W9 and the SSP Deputy, W20 , about security matters, he also testified that he did not meet directly with W5 to present his concerns about security-in-depth. Mr. Edwards, however, testified that he instead handed W5 a package of information that explained the various security issues.

310. W5 was interviewed on 19 February 2014. He testified as summarized below about the list of security deficiencies Mr. Edwards said he handed to W5 .

> I do remember a list generated of deficiencies; I do not remember [Mr. Edwards] handing me directly any files on potential security violations [on 19 March 2013]. I considered the list appropriate in the sense that [Mr. Edwards] was the head of security and his job to identify deficiencies. I do remember [discussing the list of deficiencies with my] Board of Directors (BOD) and they ... put together a POAM to address [the deficiencies] to ensure they were properly adjudicated….[44]

311. It is unclear whether W5 received the package of information directly from Mr. Edwards. Nevertheless, W5 was in receipt of the information.

312. On 4 August 2014, NAVINSGEN requested that SSP provide BOD minutes dating back to June 2011 but more importantly explain SSP's practice for briefing W5 about BOD results and actions directed. We specifically asked to know when SIPRNET issues (i.e., problems with SIPRNET in CAAs) were first raised to the BOD. W9 responded in an e-mail to the Deputy Naval Inspector General on 4 August 2014. He wrote in part:

> A meeting to discuss [any security matter like SIPRNET] would have occurred at an impromptu BOD meeting and decision minutes would not have been collected.
>
> . . .
>
> Generally all decisions regarding operations, personnel and fiscal matters are made by the 4 member BOD. When a consensus cannot be reached by the 4 member BOD, then the Director SSP is brought into the process for final adjudication. The BOD informally briefs the Director of significant matters during the Director's morning or evening daily drive by time.
>
> In January 2013, the SSP BOD was briefed for the first time by the SSP CIO and SSP security manager (Mr. Edwards) regarding potential security issues with

[44] The SSP BOD is an advisory body that was established to provide a periodic comprehensive examination of all SSP program and resource requirements in a collaborative process. The BOD considers and decides on all requested resource requirements needed to meet program responsibilities.

> the CAA and impacts on SIPRNET. The briefing recommended several options to address potential security issues. In early February 2013 the SSP BOD determined the pull back of SIPRNET to only [SSP HQ] OSS spaces. The Director was not informed of this matter until a decision was made by the BOD to pull back SIPRNET terminals, including the Director's terminal, sometime in early February 2013.

313. W5 recalled that two of the deficiencies in particular stood out among the rest; they were the SIPRNET cabling issue and the glass doors associated with spaces where classified material was stored or viewed. About these two issues he testified:

> The command made the decision to retrench SIPRNET access to the secure spaces in SP16 until physical parameters could be put in place to properly deploy it to the desktop.
>
> [The glass doors were] personally and professionally disturbing since the building was accepted from NAVFAC and it was a fairly sizable resource dollar value that we had to come up with [in order to replace them with compliant solid core doors.] Since this building is a NAVFAC/CNIC building and not under our cognizance, we had to do the funding and or coordination transfer either to NAVFAC or to CNIC. That's work in progress, we will get into the standards but I did not have the authority to instantaneously and solely direct as Director of Strategic Systems Programs. I was the Director of Strategic Systems Programs [when our offices were located] in Crystal City.

314. In his closing comments for the record, W5 testified:

> The information I want to be a part of the record is contained in my last statement is that we hired Mr. Edwards and Mr. Londagin to be the head of security and deputy security to do exactly what they did which is identify deficiencies. Having done that and presented that as part of what I consider their billet description this program has worked diligently to address those issues. Fortunately or unfortunately, the structure that I've had to work

within does not afford me with unilateral authority or sole authority so I've had to work within the constraints, financially and administratively, as the Director, SSP.

We created a POAM, worked through the POAM, and I think our believed perfect score on the Cyber Inspections on physical security reinforces that we take security seriously and our line of business require that we do so. I think they did what they were hired to do which was to point out deficiencies. This program has done what it is accountable to do which is to ensure that those deficiencies are being addressed.

With regard to [Mr. Edwards' and Mr. Londagin's unofficial and independent actions to evaluate WNY entry access controls, which were] outside of [their job] description…. At no time were [their plans to make such an evaluation] discussed with me. At no time were [they] approved by me and at no time [was their doing so] in my opinion appropriate. They were certainly outside the scope of [their] authority. Not within my authority to or theirs to execute actions outside scope [of their authority to] include surveillance of the Navy Yard, and testing the security guards. That is not within the authority I possess. I was not informed of any potential shooters. They [Edwards and Londagin] made comments how they felt but never presented any evidence because if so my comment would have been by whose authority are you doing that because it would not have been mine. I was [not] aware that they entered [WNY] gates with others ID [while conducting their own] investigation.
. . .

If I would have known through direct conversations with them or through any other means I would have stopped that because it is not within my authority or theirs to go execute.

Discussion and Analysis

315. To arrive at a conclusion about this allegation, we must determine what the Director, SSP, knew about the information and

physical security shortfalls that were identified about the SSP HQ office spaces in Building 200; determine when the Director, SSP, learned about those security shortfalls; and determine what action, if any, the Director, SSP, took or directed to be taken in response to his knowledge of any security shortfalls. As the Director, SSP, W5 was charged under the standards to ensure the proper security of the classified information under the control of the organization he led.

Official Sensitive PSA

316. On 23 March 2011, [redacted]

317. [redacted]

318. The SSP security POAM (an updated version of the list of discrepancies and corrective actions shown to NAVINSGEN team in January 2013) listed the status for building security and building unlocked 24/7 as "Not an operational requirement – however, building guards in place Jun 2013. Loading dock secured outside of normal working hours."

319. We reviewed the requirements for security-in-depth and made these observations. US requirements for security-in-depth vary according to the type of spaces being considered (CAA, OSS, etc.). There are also many levels or layers that can be utilized for security-in-depth beyond the fence line and access

to Building 200. Door alarms, cameras and swipe badges are but a few of the possible measures that could be taken. Additionally, and in accordance with SECNAV M-5510.36, the security manager, exercising the commander's authority, can specify the method for security-in-depth for each type of space. For SSP's OSS spaces the CSM is required to define the method of security-in-depth compliance on a continuation sheet to the Secure Room Checklist from CNO ltr Ser N09N2/10U213104. We found no evidence that SSP completed a continuation sheet in this case, calling into question how SSP determined or viewed their approach to meet U.S. security-in-depth requirements for their new offices in Building 200.

320. We determined that after he reported as CSM in May 2012, Mr. Edwards made thorough assessments of SSP's compliance with DON policy regarding information and physical security as it applied to SSP office spaces in Building 200. We noted an e-mail from Mr. Edwards to the Chief Information Officer, W 10 on 6 June 2012, citing concerns with CAAs and what he termed as a "massive shortfalls in some major areas." In this e-mail, Mr. Edwards listed deficiencies with glass doors in CAAs, concern with IDS monitoring (we were unable to clarify if this referred to the IDS or ACS), the requirements for X09 locks or one-inch deadbolts on CAA doors because of the lack of a building guard, and hinges and astragals that did not meet security standards. We did not find evidence of specific actions taken by SSP in response to this e-mail. We were also unable to determine to which level of seniority, above the CIO, within SSP that this information became available. Certainly Mr. Edwards had responsibility as the CSM for initiating corrective action, but we believe W 17 and W 10 also had responsibility for communicating these significant concerns up the chain of command. We have no specific evidence showing W 5 received these e-mails. As it was, these deficiencies were not corrected until March 2013 (nine months later) when SSP moved their SIPRNET cables back to OSS spaces and deactivated their CAAs.

321. There was an e-mail exchange between W 9 and Mr. Edwards on 16 October 2012 regarding a Security Newsletter and a change to SSP policies requiring personnel to "scan-in" the front door between 1801 in the evening and 0529 in the morning. We determined that this e-mail demonstrates senior SSP leader involvement in the SSP security posture and policy making. In the e-mail W 9 stated: "It's all about how we deliver the message which [makes] a huge difference in how

the message is received." This theme was repeated later on in subsequent e-mail exchanges he had with Mr. Edwards.

322. We noted also a chain of e-mails between Mr. Edwards and W9 between 20 October 2012 and November 2012 that discussed various instances where SSP personnel violated requirements for the proper protection of FOUO, Personally Identifiable Information (PII), Unclassified Controlled Nuclear Information (UCNI) and restricted SSP documents. W9 acknowledged that Mr. Edwards and W10 were doing the "right thing" in their efforts regarding security but emphasized that their means of "message delivery" needed to be focused on educating all hands to "make sure they [understood] the rules first, [before] [SSP could] begin to enforce them." This e-mail string indicated senior SSP leadership involvement, including the SSP Chief of Staff, W20 , and SSP leadership's attempts to improve SSP personnel's level of security awareness and knowledge. It also, however, documented two competing ideas:

a. A sense that the command was trying to overcome problems in their security culture ("people . . . were unaware of the rules (because they were overlooked for so long)"), and
b. A frustration between W9 (regarding methods) and Mr. Edwards (regarding his perceived lack of command support for his initiatives).[45]

323. We did not have evidence of W5 awareness of the foregoing e-mail exchange, but made the assumption that he would likely be aware of its substance because W9 directed Mr. Edwards to prepare and deliver a "security all hands presentation" for November 2012.

324. When NAVINSGEN inspected SSP in January 2013, Mr. Edwards presented a matrix of security deficiencies that included:

a. SSP's Command Security program instruction was in draft form and needed revision to conform to current security directives;

[45] SECNAV M 5510.36 Appendix A : Unclassified Controlled Nuclear Information (UCNI) - DoD or DOE unclassified information on security measures (including security plans, procedures, and equipment) for the physical protection of DoD Special Nuclear Material, equipment or facilities.

b. A lack of solid core doors on spaces designated as secure areas;
c. A lack of security-in-depth; and
d. A lack of record keeping on past security incidents.

325. The forgoing list of security deficiencies and proposed corrective actions that Mr. Edwards provided to NAVINSGEN about SSP's security issues suggested an awareness of these issues at some senior level within SSP. We know that during the NAVINSGEN inspection team's debrief in January 2013 for SSP's leadership that the inspectors commented about these security issues and that they specifically commented about SSP's ability to self-assess security issues. We determined, therefore, that W5 knew about the comprehensive list of security deficiencies and proposed corrective actions that Mr. Edwards developed.

326. On 21 February 2013, the SSP command newsletter announced SSP HQ's intentions to "increase security of SSP networks." Additionally, W9 reported that the BOD briefed W5 in February 2013 before W5 SIPRNET was pulled back from the Director's office as part of the larger SSP plan to correct its SIPRNET vulnerability issue.

327. On 1 March 2013, Mr. Edwards sent W9 an e-mail forwarding a memo entitled "security in depth determination", with the stated purpose "to make a determination if there is security in depth for the 4200 space of Building 200." The draft memo points out the issues of base access, Building 200 access, camera monitoring, entry door deficiencies, the use of PEDs within SSP spaces, and several other physical security issues. Mr. Edwards drafted a memo to be signed by the Chief of Staff, W20 , and that memo requested a security-in-depth determination be made by W5 . The discussion section of the memo recommends that "there are not sufficient layers to establish a 'yes' determination for item number 11 on [security-in-depth] on [the Controlled Access Area Checklist]." The e-mail forwarding the memo states, "this is an urgent issue no matter how long it has gone on for." W9 requested that Mr. Edwards "walk [him] thru this document." We know that during this timeframe SSP was beginning to retrench their SIPRNET cables back to the OSS spaces. We also know from W5 testimony that he was aware of a list that Mr. Edwards produced about the same time in March 2013.

328. We considered the security culture of the SSP HQ and found evidence of past weaknesses and a general lack of security focus among SSP employees. We noted that use of PEDs in secure spaces, as evidenced by testimony from SSP employees, occurred until SSP installed lockboxes and enforced PED rules. We further noted that there was an outdated command security program instruction in January 2013, more than two years after SSP relocated into Building 200. This was somewhat problematic as the outdated instruction referenced the Crystal City HQs and the protocols contained therein were not directly applicable to the relocated headquarters or SSP's current security requirements. We also considered the cultural issues that W9 raised in his e-mail exchange with Mr. Edwards wherein he commented about SSP's poor security culture and history of problems with staff knowledge about proper security. Additionally, we considered that following Mr. Edwards report of "massive shortfalls in some areas" that SSP did not file any approval for the risk as required by CNO ltr Ser N09N2/10U213104 of 16 March 2010 [Controlled Access Area Checklist]. About the foregoing, we noted that Mr. Edwards, as CSM, would most likely be the one expected to initiate such a request. We also found no evidence that SSP investigatated or made a determination of the root causes after having to retrench their SIPRNET into the OSS spaces; we determined that doing so would have been appropriate.

329. The picture that the email dialogue between Mr. Edwards and W9 (most notably) suggests is one of a command that was working to improve its security culture.

330. There were indications that leaders were aware of security shortfalls and were taking steps to correct some of the security problems that had been identified. Mr. Edwards had a strong background in security and was no doubt hired to help SSP identify and fix problems. The NAVINSGEN team noted that Mr. Edwards was proactive and capable to self-assess in January 2013. At the same time we found evidence in e-mails of some friction in relationships between the CSM and some leaders stemming not from the message, but from the CSM's method of delivery and CSM's perception that he did not have an appropriate level of leadership support for the security program. We do not intend to make judgments about these relationships, but only mean to say that it appears that friction existed.

331. We determined that SSP, including W5 , had to be aware of general weaknesses in security level of knowledge and basic practices among their personnel. We collected evidence of SSP trying to address this through actions such as the addition of the phone locker outside secure spaces in the summer of 2012 and security training in the fall.

332. We also determined that W10 and W17 were aware of what Mr. Edwards termed "major shortfall[s]," yet we did not see any evidence of an attempt at proactive resolution of these issues, which were not corrected until nine months after they were first identified and SIPRNET was retrenched and CAAs disestablished. We believe W10 and W17 had a responsibility to report these significant concerns up their chain of command.

333. We noted evidence of involvement by W9 in trying to improve SSP personnel's level of knowledge and day-to-day security practices. We also know that W9 was aware of UK security vulnerabilities in early 2011.

334. We determined that W5 had to be aware of UK security-in-depth concerns in 2011, efforts by Mr. Edwards to improve day-to-day practices in October and November 2012, and aware of the comprehensive list of security deficiencies and proposed corrective actions in January 2013. We did not obtain evidence to indicate W5 knew of Mr. Edwards's June 2012 e-mail citing "major shortfall[s]", although we believe his staff should have informed him because Mr. Edwards's concerns challenged the certification and security of all SSP CAAs. We determined issues with SIPRNET were first discovered between mid January 2013 and late February 2013 when SSP formally announced to the staff an intent to retrograde SIPRNET capability back into the SSP OSS spaces. In early 2013, this focus on SSP's security was driven by efforts to be ready for their upcoming CCRI, which, at the time, was scheduled for late March 2013. It appears that the effort to retrench SSP SIPRNET was aggressive; they moved nearly 200 terminals starting on 1 March 2013. Shortly thereafter the CAAs were deactivated and W10 certified SSP's OSS spaces, essentially removing the security problem Mr. Edwards identified in his June 2012 e-mail.

335. SSP HQ's took action to address the other physical and information security shortfalls noted by the complainants. The evidence we reviewed shows that in accordance with OPNAVINST 5530.14E, SSP HQ initiated efforts through the NDW commanding

officer to implement additional security measures for Building 200. SSP HQ took steps to replace their ACS (Nov 12); they retracted SIPRNET cables from unsecured spaces (Mar 13); they contracted for security guards to control access to Building 200 (Jun 13); and they ordered solid core doors (Nov 13) to replace the glass doors that were improperly located at the entry to spaces containing classified material. Because CAAs were disestablished; the glass doors were technically no longer a security concern.

336. Based on our analysis of the evidence we reviewed, these are the facts:

a. In accordance with DODI 5200.08 paragraphs 3 and 4, the Commander (W5) has the responsibility and authority to enforce appropriate security measures to ensure the protection of DoD property and personnel assigned, attached or subject to their control. Although he did not have responsibility or authority for access issues at the WNY or Building 200, vulnerabilities at these locations had the potential to affect SSP security plans and clearly concerned the UK personnel working at SSP based on the letter sent by W8 .

b. In accordance with SECNAV M-5239.1 commanding officers are directly responsible for identifying vulnerabilities in their operational environments and implementing the appropriate countermeasures. SECNAV M-5510.36 goes further to discuss the commander's responsibility for ensuring personnel under their commands are trained and abide by information assurance policies; further, that Commanders shall ensure that all IT assets they oversee and operate are accredited and operated in accordance with accreditation documentation.

c. In accordance with SECNAV M-5510.36, commanding officers shall ensure that all classified material is stored in a manner that will deter or detect access by unauthorized persons.

d. Several SSP Controlled Access Areas and Open Secret Storage areas were not properly certified in December 2010 and remained so through March of 2013.

e. SIPRNET was operated in SSP spaces that did not meet security requirements to support its operation from the time it was installed in 2011 through March of 2013.

f. SSP personnel routinely brought PEDs into secure spaces and used them until a new SSP policy was promulgated and enforced.

g. All of the above issues in this paragraph relating to security are within the responsibility and authority of W5 .

337. The evidence demonstrates SSP was forced into a fast paced and challenging move to an environment that did not provide the external security safeguards existing at the Nebraska Avenue and Crystal City facilities. The historic importance of the Navy Yard justifies greater public access, which imposes greater security vigilance upon individual Commands that occupy the Navy Yard.

338. Other evidence establishes the SSP Security Manager improperly certified SSP spaces upon moving into Building 200. No doubt this was a daunting task given the magnitude of the move.

339. The evidence is clear that as early as June 2012, Mr. Edwards communicated many physical security concerns to W10 , W17 , and to others within the SSP organization who should have brought these matters to W5 attention. Mr. Edwards' e-mail was a critical opportunity. Our review of the certification checklist for CAAs revealed that Mr. Edwards' concerns were valid; however, we found no definitive action in response to his e-mail.

340. Despite this determination, W5 was not relieved of the responsibility for security outlined in the governing DoD and SECNAV manuals. Under Article 0802 of the U.S. NAVY REGULATIONS, the responsibility of the commanding officer for their command, is "absolute." We accept that exercising this command authority in the context of the WNY and Building 200 is not without its significant challenges. W5 was not responsible for, nor did he have authority over, WNY access procedures or Building 200 access. Additionally, W5 was in charge of a large organization in which there are SSP personnel designated to lead and manage security, IT, and the

day-to-day operation of the organization he was responsible for. Clearly those personnel also bear responsibility for the security shortfalls we have identified in this report, especially the CSM at the time of SSP's occupation of Building 200 and not reacting to Mr. Edwards' June 2012 e-mail. We determined, by a preponderance of evidence, that all security requirements specified by the applicable standards were not in place during the period December 2010 and March 2013. Consequently, we must conclude that W5 , as the organizational commander, did not meet his responsibility to ensure these vulnerabilities were identified and prevent the violation of information security procedures. Importantly, we noted aggressive action by SSP in Febraury and March 2013 to bring their CAAs and SIPRNET into compliance. We also noted that in January 2014, FCC reviewed SSP's physical and information security, and assigned a risk indicator of "low" and a grade of "Excellent." Finally, we found no evidence of compromise or loss of classified material.

Conclusion

341. The allegation is **substantiated.**

Recommended Actions

342. SSP continue to stress day-to-day security protocols and standards as an all hands responsibility.

343. If intentions are to recertify CAAs, SSP should bring in Fleet Cyber Command experts and other physical security and information security experts to pre-check and later assist in certification of CAAs.

344. Incorporate command security POAM review in all BOD meetings until remaining administration and training items are completed.

345. SSP consider adjusting BOD membership to include the SSP CIO and CSM.

346. SSP should thoroughly review and investigate security violations or possible compromises to determine root cause and take appropriate and timely corrective action.

Actions Planned or Taken

347. SSP reported to NAVINSGEN that all security deficiencies alleged by the complainants associated with SSP spaces in Building 200 have been corrected. To summarize SSP HQ:

a. Took steps to replace their ACS (completed November 2012);
b. Retracted SIPRNET cables from unsecured spaces (completed March 2013);
c. Contracted for security guards to control ingress and egress of Building 200 (completed July 2013);
d. Properly certified all spaces (completed March 2013);
e. Ordered solid core doors to replace the glass doors that were improperly located at the entry to spaces containing classified material (completed November 2013); and
f. Installed lock boxes for PEDs (completed June 2013) and upgraded their PED policy (completed November 2013).

Notes: 1) Once SSP retracted SIPRNET cables, the glass doors were no longer a security issue; however, SSP intended to replace these doors to allow re-designation of the affected spaces. 2) SSP contracted security guards for Building 200 to add an additional layer of security and to support UK security requirements.

348. In January 2014, SSP passed a FCC Cyber Readiness Inspection that reviewed information and physical security with strong grades.

349. During this investigation, SSP provided NAVINSGEN with a security POAM that lists outstanding and recurring actions. These primarily consist of administrative actions, recurring training and broader efforts to coordinate with the WNY and NDW for periodic vulnerability and risk assessments surveys.

APPENDIX A – FINDINGS BY ALLEGATION

Allegation One

1. The governing law for entering military, naval, or coast guard property is found in 18 U.S.C. § 1382 and any violation of defense property security regulation is found in 50 U.S.C. § 797. The regulatory basis for physical security and access control on DoD installations is found in DoD Instruction (DoDI) 5200.08 CH-1, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB), of 10 December 2005; and DoD 5200.08R CH-1, Physical Security Program, of 27 May 2009.

2. 18 U.S.C. § 1382 provides that "Whoever, within the jurisdiction of the United States, goes upon any military, naval, or Coast Guard reservation, post, fort, arsenal, yard, station, or installation, for any purpose prohibited by law or lawful regulation... Shall be fined under this title or imprisoned..."

3. 50 U.S.C. § 797 provides that "... a defense property security regulation is a property security regulation that, pursuant to lawful authority in (2)(A) shall be or has been promulgated or approved by the Secretary of Defense (or by a military commander designated by the Secretary of Defense or by a military officer, or a civilian officer or employee of the Department of Defense, holding a senior Department of Defense director position designated by the Secretary of Defense) for the protection or security of Department of Defense property." It further states in (3)(B) that a property security regulation is a regulation that, "otherwise [provides] for safe guarding such property against destruction, loss, or injury by accident or by enemy action, sabotage, or other subversive actions."

4. DoDI 5200.08 provides that DoD installations, property and personnel shall be protected and that applicable laws and regulations shall be enforced. It provides the authority of a DoD commander to take reasonably necessary and lawful measures to maintain law and order and to protect installation personnel and property. Chapter 3, section 3.2.2, states the DoD authority includes "the removal from, or the denial of access to, an installation or site of individuals who threaten the orderly administration of the installation or site." And Chapter 3, section 3.2.3, states the authority, "Shall not be exercised in an arbitrary, unpredictable, or discriminatory manner."

5. DoDI 5200.08, Chapter 3, section 3.2.4, permits prohibiting individuals from reentering an installation after they have been removed and ordered not to reenter under 18 U.S.C. § 1382. If this order is violated, the commander of a DoD installation may detain individuals not subject to military law until the civil authorities may respond. Offenders may be appropriately prosecuted in accordance with the law.

6. DoD 5200.08R implements the policies and minimum standards for the physical security of DoD installations and resources. Chapter 3, section 3.1, states that "Access control is an integral and interoperable part of DoD installation physical security programs. Each installation commander/facility director must clearly define, consistent with DoD policy, the access control measures... required to safeguard personnel, facilities, protect capabilities, and accomplish the mission."

7. DoD 5200.08R, Chapter 3, section 3.3.1, states "Homeland Security Presidential Directive-12 (HSPD-12), mandates policy for a common identification standard for all Federal employees and contractors."

8. DoD 5200.08R, Chapter 3, section 3.3.1, further states that "The Federal Information Processing Standard 201-1 (FIPS 201-1) provides standards for the identity verification, issuance, and use of the common identity standard. The DoD Federal Personal Identity Verification credential, the Common Access Card (CAC), will provide a level of identity assurance and a method of authentication. The CAC shall be the principal identity credential for supporting interoperable access to installations, facilities, buildings, and controlled spaces. The CAC, upon presentation at perimeter security locations, shall be accepted for perimeter screening purposes."

9. DoD 5200.08R, Chapter 3, section 3.3.1.4 states, "Occasional visitors to Federal facilities will continue using a locally established, temporary issue, visitor identification system."

10. SECNAV M-5510.36, Department of the Navy Information Security Program, of June 2006, provides physical security requirements for the protection of classified information.

11. OPNAVINST 5530.14E CH-1, Navy Physical Security and Law Enforcement Programs, of 19 April 2010, implements DoD physical security and law enforcement policy, and requires installation

commanding officers to establish and maintain a Navy Security Program that implements higher headquarters requirements.

12. Commander, Navy Installations Command (CNIC) instruction, CNICINST 5530.14A, CNIC Ashore Protection Program, of 29 May 2013, implements the OPNAV physical security and law enforcement requirements for all Navy installations. The physical security and law enforcement programs safeguard personnel, property and material by enforcing rules, regulations, and law at Navy installations and activities.

13. The Under Secretary of Defense, DTM 09-012, Interim Policy Guidance for DoD Physical Access Control, establishes DoD access control policy and the minimum DoD security standards for controlling entry to DoD installations. DTM 09-012 implements the requirements of the HSPD-12 and the CNICINST 5530.14A implements DoD access control requirements and promulgates access control standards for all Navy installations.

14. WNY is the U.S. Navy's oldest shore establishment and houses the Naval Historical Center to include the Display Ship BARRY, the Navy Museum, the Navy Art Gallery, the Navy Library and holds many ceremonial events in Leutze Park. In addition to the historical element, the official residences of CNO and other senior Flag Officers are located on the WNY and the WNY and is home to numerous support activities for the fleet and aviation communities. As a matter of policy the DoD has determined that many features of the WNY should be open to the general public.

15. The DTM 09-012 states that access control standards shall include identity proofing, vetting to determine the fitness of an individual requesting and/or requiring access to installations, and issuance of local access credentials. All unescorted persons entering DoD installations must have a valid purpose to enter, have their identity proofed and vetted, and be issued, or in possession of, an authorized and valid access credential. The DTM 09-012 references the DoD instruction and regulations cited above.

16. The DTM 09-012 provides that visitors to the WNY who do not possess a CAC have their identity verified and vetted at the Pass Office prior to being issued an unescorted installation pass. Visitors must provide an authorized form of identification, e.g., driver’s license. Their need for access is validated by the Pass Office that also vets visitors by using an authorized data source (The National Crime Information Center database (NCIC)) to perform a criminal background check.

17. The Judge Advocate General Manual (JAGMAN) Report of Investigation into the Fatal Shooting Incident at the Washington Navy Yard (WNY) on 16 September 2013 and Associated Security, Personnel, and Contracting Policies and Practices, 5800 N00ND of 2 November 2013, inquired into all aspects of security employed by NSAW, WNY. The JAGMAN investigation referenced local NSAW regulatory requirements established in NSAW 5560.1, Naval Support Activity Washington Traffic Policy, and NSAWINST 5532.1, Procedures for Vetting Visitors to Navy Museum on the WNY. SECDEF also directed an "internal review of the Washington Navy Yard shooting" conducted by the Under Secretary of Defense for Intelligence, dated 20 November 2013.

18. The time period reviewed by the JAGMAN investigation does not correlate to the time period of the OSC allegations. However, the security concerns raised by the OSC complainant were examined in the JAGMAN investigation and concluded to be not in compliance with the methods and practices of access control.

19. With respect to access controls at the WNY, the JAGMAN investigation concluded in Chapter 4, Finding 4.3, [redacted] Official Sensitive PSA

20. The JAGMAN investigation, Chapter 4, page 81, Fundamentals of Access Control, defined the objective of access control for entrance to installations with and without a DoD-issued CAC. Military, civilian, and contractors possessing DoD-issued CACs have their identity verified at the card issuance site and vetted according to applicable DoD personnel security standards. As such, military, civilian, and contractors possessing a CAC can properly gain access to installations via either an electronic physical access control system or through a manned security post.

21. Visitors who do not possess a CAC, have their identity verified and vetted at the Pass Office as previously described. Visitors must provide an authorized form of identification. Their need for access is validated by Pass Office personnel, who also vet visitors by using NCIC background check.

22. As stated above, the JAGMAN investigation concluded that methods and practices employed to vet unescorted visitors at the WNY were not in compliance with local, DON and DoD instructions.

23. The JAGMAN investigation, Chapter 4, section 4.3.1 also included the following information.

:

Official Sensitive PSA

[redacted]

25. W6 was the SSP CSM when SSP HQ moved into office spaces in Building 200 on the WNY. She was responsible for certifying that SSP HQ spaces in Building 200 met the physical security requirements of SECNAV M-5510.36.

26. W6 supervisor, W7 received information in February 2011 concerning security vulnerabilities related to the WNY gate access controls. A 23 March 2011 letter from W8 , Deputy Strategic Programs Royal Navy Branch (SP50), to W9 , SSP Director, Plans and Programs (SP10), references an e-mail dated 22 February 2011, wherein W7 shared WNY access control vulnerability information with W8 SP50 (Uk unit) is also located in Building 200.

Official Sensitive PSA

[redacted]

W10

28. On 25 April 2011, , Management Information and Support Services Branch Head, sent a memo to W9 via W6 and W7 , titled "SP50 Washington Navy Yard Physical Security Concerns," that addressed SP50's security-in-depth concerns. [redacted]

Official Sensitive PSA

29. On 20 July 2011, W9 sent an e-mail to W11 , Naval District Washington about the physical security and WNY access control issues. W9 copied W5 , W12 , W13 , W10 and W6 . W9 stated, [redacted]

Official Sensitive PSA

[redacted] keholders to socialize a plan for security modifications.

30. As early as 20 July 2011, the DIRSSP was aware of security-in-depth and WNY access concerns based upon W9 e-mail.

31. On 1 September 2011, W9 again e-mailed W11 to follow-up on his 20 July 2011 e-mail. W9 copied W5 , W12 , W13 , W10 and W6 .

32. Mr. Edwards, SSP CSM, testified that he was appointed to his position on 29 June 2012 and shortly thereafter, used the credentials of his Deputy, Mr. Vernon Londagin, on one occasion to gain access to the WNY. He stated that Mr. Londagin was a

passenger in the vehicle at the time. Mr. Edwards stated, "... So we did. I got his [Mr. Londagin's] ID one time to see how we'd get on. Well, we asked them, What if I come through because they're only checking the driver. They don't check anybody else in the car." Mr. Edwards contended that he was allowed on the WNY without an adequate identification check since the identification he presented was Mr. Londagin's. He asserted that the credentials he presented were not reviewed properly and that he used the credentials of a passenger in the vehicle while his credentials as the driver, were not properly checked.

33. Mr. Edwards testified, "What happens, they're taking – you're required – taking the card and inspecting the expiration date and ensuring it is an actual CAC card, handing it back after you make positive identification to the person that's driving, and giving it back to them. That's how they're supposed to check and they're required to check." He stated, "So how can I use that as defense in depth was my thing if I'm using his ID and they see it's me? ... People were coming in with other cards, other forms."

34. Mr. Edwards also testified that at the same time his car did not have a Naval District Washington decal. He stated, "At that time, decals were required or you're supposed to go to the visitor gate. Anybody was getting on with a driver's license." Mr. Londagin, who was interviewed at the same time, stated, "Yeah, the military personnel were pretty spot on when it came to the decal thing and checking the CAC cards or whatever. The security guards that aren't military, they don't care."

35. In a Memorandum of 18 March 2011, Assistant Secretary of the Navy (Energy, Installations and Environment), formerly ASN(I&E), eliminated the requirement for vehicles entering DON installations to be registered via vehicle decals (DD Form 2220).

36. CNO WASHINGTON DC NAVADMIN 146/13 of 29 May 2013 promulgated additional Navy policy eliminating the requirement for vehicle decals for base access, effective 1 July 2013.

37. To clarify the use of vehicle decals by NSAW between March 2011 and May 2013, NAVINSGEN NR-106 Operations Officer, W14 was consulted as a Security Subject Matter Expert. In his civilian capacity, W14 is the CSM for Military Sealift Command and was certified up to Security Program Integration Professional Certification through Defense

Security Services in 2013. W 14 stated that prior to issuance of the NAVADMIN; decals for NSAW were required mainly for parking management. To obtain a decal, a driver had to visit the Pass Office and provide a valid license and registration as well as proof of insurance even if they possessed a CAC.

38. Aside from the complainants' testimony, we were unable to develop evidence concerning the specifics of the one particular event when Mr. Edwards used Mr. Londagin's credentials to access the WNY.

39. Mr. Edwards testified that he observed people entering the WNY unescorted at a gate using "other cards" or "other forms." He stated, "... anybody with a driver's license was coming on unchecked." Mr. Edwards provided no additional detailed information when questioned as to how he was aware what type of card was being used to gain access to the WNY.

40. We were unable to develop evidence to support or refute Mr. Edwards' allegation that people entered a WNY gate unescorted using other cards or a driver's license. The JAGMAN investigation did conclude that the methods and practices employed to vet unescorted visitors were not in compliance with local, DON and DoD instructions. The JAGMAN investigation stated that the WNY implementation of physical security and access control policies was being further reviewed. While the JAGMAN investigation did find deficiencies in the procedures, it did not identify the use of "other cards" or "other forms" of identification as an issue of concern.

41. In his interview, Mr. Edwards alleged that when he raised his concerns regarding the leniency of WNY entry procedures, the WNY Pass Office advised that because a museum and credit union were located on the WNY, only a driver's license or state identification card was required for base entry.

42. NAVINSGEN verified through W 14 that prior to 16 September 2013, pedestrian access onto the WNY required a driver's license, state or federal identification. Visitors accessing the WNY in vehicles, presenting a driver's license, state or federal ID, with no CAC, required vetting through the Pass Office to obtain a temporary vehicle pass. The vetting for a temporary vehicle pass required a valid state license, current vehicle registration and proof of vehicle insurance and a valid purpose to enter. Vehicles could enter onto the WNY without a proper DoD decal; however, it was required that a valid driver's

license, current proof of vehicle insurance and registration, or a rental car agreement that verified proof of vehicle insurance be presented.

Allegation Two

43. SSP HQ was previously located in the NAC Washington, DC, and then moved to Crystal City, Arlington, Virginia. By direction of the Deputy ASN(I&E), SSP relocated to the WNY, Washington, DC, in December 2010. Prior to the move, Public Law 108-268 directed NAVFAC to repair, restore and modernize Building 200, WNY, for SSP occupancy.

44. SSP HQ occupied Building 200 spaces in December 2010. W6 was the SSP CSM at that time.

45. In accordance with SECNAV M-5510.36, on 21 December 2010, W6 certified Suite SP205, Room 4200, as a SR authorized for personnel cleared to the level of information being processed; SR referred to as Open Storage Secret Area (OSS) throughout the remainder of this report.

46. On 3 March 2011, W6 certified that Suite SP202, Room 5318 was certified as OSS for classified meetings at the level of Top Secret and below in accordance with SECNAV M-5510.36.

47. On 5 August 2011, W6 certified that Rooms 4103 and 4103A were inspected and met the physical standards of SECNAV M-5510.36. She advised that they were designated as OSSs/CAAs authorized to handle and process classified materials up to the level of Top Secret.

48. SECNAV M-5510.36, Section 10-3, provides that "[c]lassified information not under the personal control or observation of an appropriately cleared person shall be guarded or stored in locked GSA-approved security container, vault, modular vault, or secure room (OSS)." In an OSS, classified information can be stored openly rather than in GSA-approved containers or vaults when not in use. In addition, in an OSS, SIPRNET does not require a Protected Distribution System (PDS).

49. SECNAV M-5510.36, Exhibit 10, provides construction standards for the approved storage areas noted above. To certify a room as OSS, SECNAV M-5510.36 includes direction pertaining to: 1) how the walls, floors, roofs, ceilings, windows, and doors are to be constructed; 2) what types of locks

and hardware are required on the doors; 3) the size of utility openings; 4) access control; and 5) other security measures such as security-in-depth requirements, lock boxes, GSA-approved security containers for storage of classified information, inspections of the spaces by guards, and the use of an IDS.

50. The following sections in SECNAV M-5510.36, Exhibit 10A, are relevant to this allegation pertaining to OSSs:

> 2. SECURE ROOM
>
> a. Walls, Floor, and Roof. The walls, floor, and roof construction shall be of permanent construction materials; i.e., plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other materials offering resistance to, and evidence of unauthorized entry into the area. Walls shall be extended to the true ceiling with permanent construction materials, wire mesh, or 18-gauge expanded steel screen.
>
> b. Ceiling. The ceiling shall be constructed of plaster, gypsum, wallboard material, hardwood, or any other acceptable material.
>
> c. Doors. The access door to the room shall be substantially constructed of wood, metal, or other solid material and be equipped with a built-in GSA-approved combination lock meeting Federal Specification FF-L-2740... When double doors are used, an astragal will be installed on the active leaf of the door. The hinge pins of outswing doors shall be penned, brazed, or spot welded to prevent removal. Doors other than the access door shall be secured from the inside (for example, by a dead bolt lock, panic dead bolt lock, or rigid wood or metal bar which extends across the width of the door), or by any other means that will prevent entry from the outside. Key operated locks that can be accessed from the exterior side of the door are not authorized. Each perimeter door shall be protected by a balanced magnetic switch that meets the standards of UL 634.

51. The following sections in SECNAV M-5510.36, Exhibit 10D, are relevant to this allegation:

> 1. IDS. An IDS must detect an unauthorized or authorized penetration in the secure area. An IDS complements other physical security measures and consists of the following:

a. Intrusion Detection Equipment (IDE)
b. Security forces
c. Operating procedures

. . .

3. THREAT, VULNERABILITY, AND ACCEPTABILITY

a. As determined by the commanding officer, all areas that reasonably afford access to the container, or where classified data is stored should be protected by an IDS unless continually occupied. Prior to the installation of an IDS, commanding officers shall consider the threat, vulnerabilities, in-depth security measures and shall perform a risk analysis.

52. On 7 May 2009, the CNO issued "Interim Policy Changes, Reminders, and Clarifying Guidance to SECNAV M-5510.36" mandating that OSSs be constructed per Exhibit 10A. Although CAAs, and Restricted Access Areas (RAAs) shall be designated in writing by the CSM and shall comply with the requirements in the CNO/U.S. Marine Corps (CNO/USMC) IA-PUB 5239-22 of September 2008, "IA Protected Distribution System (PDS) Publication."

53. In addition, on 16 March 2010, CNO issued another "Interim Policy Change to Requirements for a Secure Room used for Open Storage Secret and Designation of Secure Rooms, Controlled Access Area and Restricted Access Area." The policy change updated requirements regarding authorized supplemental controls required for an OSS and mandated the use of a template letter and updated checklists for adequate protection of classified material.

54. On 11 March 2011, W6 certified all SSP HQ spaces within Building 200 as CAAs. In doing so, she certified that the physical environment of SSP HQ spaces provided adequate protection for processing classified information and met the physical security requirements of SECNAV M-5510.36.

55. A CAA has less stringent security requirements than an OSSs. Per the Information Assurance Publication (IA PUB)-5239-22, dated September 2008, Section 2.2., it is a "physical area (e.g., building, room, etc.) which is under physical control and to which only personnel cleared to the level of the information being processed are authorized unrestricted access." All other individuals are either escorted by authorized personnel or are under continued surveillance. Within a CAA, a PDS is not

required for classified information processed at or below the classification level to which access to the CAA is controlled. While unprotected SIPRNET cables may run within the CAA, IA [Information Assurance] PUB-5239-22 mandates that they cannot run outside the perimeter of the CAA in a space certified at a lower standard.

56. To certify a room as a CAA, IA PUB-5239-22 includes direction to: 1) how the walls, floors, roofs, ceilings, windows, and doors are to be constructed; 2) what types of locks and hardware on the doors are required; 3) the size of utility openings; and 4) access control. It also includes other security measures such as lock boxes, GSA-approved security containers for storage of classified information, and the use of an IDS.

57. The following specific sections in IA PUB-5239-22 are relevant to this allegation pertaining to CAAs:

> 4.2. (U) Walls, Floor and Roof
>
> (FOUO) CAA: The walls, floor, and roof construction shall be of permanent construction materials (i.e., plaster, gypsum, wallboard, metal panels, hardboard, wood, plywood, or other materials) offering resistance to and evidence of unauthorized entry into the area. Walls shall be extended from true floor to true ceiling with permanent construction materials or 18-gauge expanded steel screen. If the walls cannot be extended, then an intrusion detection system shall be installed to monitor the space above the terminal room.
>
> 4.3. (U) Doors
>
> (FOUO) CAA: The access door to the area shall be substantially constructed of wood, metal or other solid material. The door shall be secured with a lock meeting FF-L-2890 specifications or, depending upon the security-in-depth, a lock meeting UL-437 security requirements subject to the Service [Designated Approving Authority] DAA approval. The request for waiver of a FF-L-2890 lock on the CAA door will be submitted by the command with the CTTA evaluation of the security-in-depth prepared by the Security Manager or Physical Security Officer to the Service DAA. Note: CAAs approved prior to issuance of this

publication do not require the immediate installation of the FF-L-2890 lock unless the CAA is subject to remodeling or upgrade. These CAAs shall be brought to full compliance by the end of Calendar Year (CY) 10. The hinge pins of out swing doors shall be penned, brazed, or spot-welded to prevent removal. When double doors are used, an astragal will be installed on the active leaf of the door. Doors other than the access door shall be secured from the inside (i.e. by a dead bolt lock, panic dead bolt lock, or rigid wood or metal bar which extends across the width of the door), or by any other means that will prevent entry from the outside. Procedures shall be established to ensure that doors are secured at the end of the workday. During working hours the terminal area shall be: (1) occupied; (2) accessible through the use of a cipher or simplex(r) lock, or a swipe badge system; or, (3) have the doors locked when unoccupied.

4.4. (U) Windows

(FOUO) CAA: All windows which might reasonably afford visual observation of classified activities within the facility shall be made opaque or equipped with blinds, drapes, or other coverings. Windows that are less than 18 feet above the ground measured from the bottom of the window, or are easily accessible by means of objects directly beneath the windows, will be locked at all times. The locking mechanism and window construction shall be such as to provide indications of any attempt of forced entry. If the window construction is inadequate to provide said indication, then protective coverings, such as bars, need to be placed over the windows. The protection provided to the windows need be no stronger than the strength of the contiguous walls. Windows containing climate control units (e.g., air conditioners) must be secured in a manner to provide indications of any attempt at forced entry.

58. W6 remained the SSP CSM until she retired in December 2011.

59. In May 2012, SSP hired Mr. Edwards as the new SSP CSM. Mr. Edwards testified that, upon assuming his duties, he observed the SSP HQ spaces and reviewed the certification paperwork left behind by W6 . He conducted his

own internal inspection of SSP HQ spaces to determine if they complied with security requirements contained in SECNAV M-5510.36. He also noted that W 6 either used the wrong checklists or did not complete checklists when conducting her inspections. Mr. Edwards determined that SSP HQ spaces did not comply with CAA and OSS requirements set forth in SECNAV M-5510.36. He opined in his testimony that W 6 falsified information in her certification of SSP HQ spaces, confirming that they met the physical security measures required by SECNAV M-5510.36 when in fact they did not.

60. On 6 June 2012, Mr. Edwards sent an e-mail to W 10 , Management Information and Support Services Branch Head, advising him that although all of SSP HQ was designated as a CAA, he found deficiencies in CAAs and OSSs. He noted the following in his e-mail:

a. That the glass doors were not made of wood, metal, or some other solid material and were in violation of IA [Information Assurance] PUB-5239-22.4.3.;
b. That the doors possessed clear windows, and therefore, provided views for observation in violation of IA PUB-5239-22.4.4.;
c. That the IDS was not monitored in violation of IA PUB-5239-22.4.2.;
d. That, because there was no building guard, the doors had to possess X09 locks or 1 inch deadbolts IA PUB-5239-22.4.3.;
e. That the door hinges were not correctly installed on the inside of the doors, and therefore, were required to be pinged or welded, which was not the case, in violation of IA PUB-5239-22.4.3; and
f. That all the double doors were required to have astragals installed on them but did not, in violation of IA PUB-5239-22.4.3.

61. On 27 August 2012, SSP hired Mr. Vernon Londagin as Deputy, Physical Security Manager to assist Mr. Edwards. Mr. Londagin corroborated Mr. Edwards' testimony that SSP HQ spaces, during the time of his employment with SSP, did not comply with SECNAV M-5510.36. Mr. Londagin stated that he also noted the numerous deficiencies in the building that Mr. Edwards described when he came on board.

62. From 23 to 31 January 2013, NAVINSGEN conducted a command inspection of SSP HQ, during which the inspectors spoke to Mr. Edwards. The NAVINSGEN Command Inspection Report of SSP, dated

12 June 2013, stated that at the time of the inspection, Mr. Edwards was on board eight months and had conducted a self-assessment of SSP spaces. NAVINSGEN found that, during his self-assessment and follow-up evaluation, Mr. Edwards noted:

a. Gaps in physical and information security;
b. Lack of a functioning IDS (Mr. Edwards clearly told NAVINSGEN inspectors the SSP IDS was malfunctioning, and our report indicated the IDS malfunctioned. We were unable to confirm whether Mr. Edwards meant IDS or ACS);
c. Lack of solid core doors on spaces designated as secure areas;
d. Lack of recordkeeping on security incidents; and
e. A need to draft a new instruction and Emergency Action Plan to improve overall security awareness and practices. The NAVINSGEN report verified the deficiencies and that SSP had developed a plan of action to address these issues. This plan of action included updating instructions, emergency action plans, increasing security awareness, and proactive efforts to mitigate security shortfalls.

63. On 24 January 2013, NAVINSGEN inspectors met with SSP employees, W 10 , Mr. Edwards, Mr. Londagin, and W 16 Special Security Representative, SSP HQ. NAVINSGEN meeting notes indicate that SSP HQ participants advised that the alarm system for the entire WNY was outdated and grossly inadequate. Mr. Edwards stated that over 250,000 alarms went off over the 18 months, with most being phantom alarms, and because of the numerous false alarms, the alarm was currently masked. The SSP employees reported that SSP had purchased and was currently installing a new ACS for Building 200 to replace the malfunctioning ACS in place when SSP occupied Building 200.

64. W 17 , SSP Chief Information Officer (CIO), testified when Mr. Edwards first arrived in May 2012, he identified a number of interior doors within SSP HQ CAAs that were made of wooden frames, but a large portion of the center of the door was constructed of glass. Mr. Edwards advised that this construction was not in compliance with SECNAV M-5510.36. Mr. Edwards advised W 17 that he tested one of the doors by attempting to break it with a hammer. Although the glass was shatterproof and did not break, the wood strip around the side of the door broke off quickly, which did not meet security requirements. Mr. Edwards reported to W 17 that he was also concerned with the glass and the fact that it was clear.

He stated this was in violation of security requirements. He noted that a bystander outside the CAA could observe a Secret safe in a CAA from outside the door. Accordingly, W 17 advised that Mr. Edwards placed white opaque coverings over the entire inside glass to make it impossible to see through and increase the level of security.

65. W 14 testified that, after the NAVINSGEN Command Inspection of SSP, Mr. Edwards contacted him and invited him to SSP HQ to discuss SSP HQ's physical security. W 14 stated that he met with Mr. Edwards, and did a walk-through of SSP HQ spaces. He described that SSP HQ had a number of doors leading to their CAAs that were constructed of 75 percent glass in the center with a wooden frame. As these doors led to passageways and office spaces, he opined that they did not comply with IA PUB-5239-22, which required a door constructed of a solid material like wood or metal. W 14 testified that anyone without a clearance could look down the hallway and see into the CAAs.

66. W 14 also noted that in checking a designated OSS room, they were able to push up the drop ceiling. Also, they found that the wall was not a floor-to-ceiling wall as required by the security regulations. He advised that they could see over the bulkhead, making it an unsecure space. W 14 stated that he believed SSP HQ took measures to correct that issue immediately after their walkthrough to ensure the wall was floor-to-ceiling. On 30 July 2014, W 14 confirmed by way of a walkthrough of SSP HQ's spaces that the issue had been resolved and the OSS met all security requirements.

67. W 14 corroborated W 17 testimony that he was present when Mr. Edwards and Mr. Londagin attempted to shatter the glass and that, although the glass was shatterproof, the surrounding wooden frame broke easily. W 14 testified that he discussed with Mr. Edwards the need to at least cover the glass portion with an opaque window covering to prohibit anyone from looking through the pane and make it more secure. This, W 14 surmised, was an interim measure to heighten security until the doors could be replaced.

68. W 18 , a contractor for JRC Integrated Systems, testified that during Mr. Edwards' tenure at SSP HQ the double doors on OSSs in building 200, which are required to have astragals, were deficient. She reported that this deficiency was corrected but did not relate when the correction occurred.

69. W 16 Special Security Representative, SSP, testified, between May 2012 and March 2013, there were deficiencies with CAAs and OSSs to include the lack of a metal strip between double doors and visitor logs not being properly updated. He related that, although the visitors' identifications were checked, the logs were not adequately maintained. W 16 stated that SSP worked to correct the deficiencies but did not elaborate on what corrections were made or when they were completed.

70. Mr. Edwards and Mr. Londagin testified that in January 2013, SSP HQ leadership requested Mr. Edwards sign checklists and other documentation in preparation for an upcoming Fleet Cyber Command (FCC) Cyber Command Readiness Inspection (CCRI) certifying that SSP HQ spaces complied with security requirements. Mr. Edwards testified that he refused to sign the documents. Mr. Londagin further testified that while Mr. Edwards was out of the office he was requested to sign the documents in Mr. Edwards' absence. Both men advised that they refused to sign the documents because spaces did not comply with Navy security requirements. Mr. Londagin testified that they would not go to jail for signing documents which he knew to be incorrect.

71. On 1 March 2013, Mr. Edwards sent an e-mail to W 9 , and attached a copy of the CAA Checklist he had completed. He copied W 10 , W 19 , Deputy Director, Plans and Programs Division, and W 20 , Deputy Director, SSP, on the e-mail. In the attachment, Mr. Edwards outlined a number of deficiencies found with regard to SSP HQ physical security. The issues identified were as follows:

a. Anyone can access the base with a driver license;
b. No checks are done on those who enter the base physically or electronically;
c. Building 200 is unlocked at all times;
d. Building 200 has numerous rooms that one could hide in or conceal themselves at any time as they are unsecure at all times;
e. IDS in Building 200 does not work as it does not work more specifically in the 4200 space;
f. CCTV system is not monitored;
g. Cleared guards are not controlling or patrolling inside of Building 200 spaces;
h. Entry doors in Building 200 are not built to Physical Security requirement standards;

i. Doors do not have proper sophisticated locks installed on them;
j. Access control/deterrent hardware such as astragals is not present on doors in SSPHQ spaces;
k. No penetration testing has ever been conducted;
l. All SSP spaces are easy to penetrate undetected and exit with no evidence of penetration (Entrance can be made in less than 1 minute);
m. No threat assessment has been conducted on the building and it is an exterior barrier to the base;
n. Spaces within building 200 are easily monitored from the exterior and interior of the building;
o. Any and nearly all types of electronic devices may be found within SSPHQ spaces such as iPads, Personal Computers, WiFi cards, iPods, iPhones and etc.;
p. Access control for visitors is not adequate;
q. The fence on both sides of Building 200 is easily scaled and no guards posted for the majority of the day; and
r. No former accreditation packets were on file and spaces have been operating improperly for multiple years.

On the same date, W 9 responded by e-mail, directing Mr. Edwards to see him on the next Monday to discuss the issues and walk through the document.

72. On 5 March 2013, Mr. Edwards sent an e-mail to W 9 and attached a spreadsheet containing SSP HQ issues, which included the solution and the status of the action being taken for each deficiency. The list stated that no entry doors had CDX09 locks and no double doors contained astragals. In addition, he noted that the OSS and CAA packets were done incorrectly or missing. For all of these deficiencies, Mr. Edwards noted that they were being worked.

73. On 18 March 2013, Mr. Edwards sent an e-mail to W 10 advising that he had informed the command that the following problems existed:

a. No adequate means to protect SIPRNET required;
b. No PDS existed for SIPRNET or lock boxes;
c. SSP HQ did not have a current designated CAA for the SIPRNET lines running throughout the command and certain areas had active network ports;
d. Room 205 was not designated an OSSs or a CAA;
e. There was no kill switch on the SIPRNET; and

f. Physical security requirements were ignored even by the head office as SIPRNET is viewed and used with windows up and left logged-on when not monitored.

In his e-mail, he opined that there should currently be no SIPRNET in the SSP HQ. He also requested notification in writing, if the command was altering security requirements; which he believed was a "large scale security violation."

74. Mr. Edwards testified that over his tenure at SSP HQ he spoke primarily with W 20 and W 9 regarding his security concerns. He reported that in March 2013, he asked to speak directly with W 5 to put him on notice of the existing security violations. Mr. Edwards testified that, on 19 March 2013, he met with W 5 to discuss his concerns regarding security. Mr. Edwards alleged he handed W 5 a file and advised that he wished to discuss his security concerns. W 5 testified, "I do not remember him [Mr. Edwards] handing me directly any files on potential security violation."

75. By letters dated 20 March 2013, W 10 certified that Rooms TC-42, 4103, 4103A, and 4200 in building 200 were certified and designated as secure rooms for OSS.

Allegation Three

76. In addition to the findings of this allegation, the findings, analysis and conclusions of Allegation Two are adopted.

77. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), of 9 February 2011, established that the Services were required to review and implement required Security Technical Implementation Guides (STIGs), National Security Agency (NSA) security configuration guides and industry best practices to ensure DoD standard security configuration. CJCSI 6510.01F references National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 7003, of 13 December 1996, Protected Distribution System, as a source document for PDS requirements.

78. CJCSI 6211.02D, Defense Information Systems Network (DISN) Responsibilities, of 24 January 2012 requires the Services, with respect to classified data, to ensure an Authorizing Official (AO) validates all requirements to tunnel classified information across unclassified Internet Protocol (IP) infrastructure and if

not, requires approval before tunneling classified data across unclassified IP infrastructure.

79. STIG CS-040, updated 5 May 2008, references the NSTISSI No. 7003, and states that classified information shall be transmitted by electronic means over an approved secure communications system authorized by the Director NSA for PDS designed and installed to meet the requirements of NSTISSI No. 7003. This STIG applies to voice, data, message (both organizational and e-mail), and facsimile transmissions. As per the STIG CS-040 and NSTISSI No. 7003, a PDS is required for any unencrypted classified data transfer, which is NOT contained within an area of classification equal to the data or higher. Secret data transfer must be protected by PDS if not within a SECRET CAA or higher.

80. CNO/USMC IA PUB-5239-22 established that while unprotected cables [SIPRNET] may run within a CAA, they may not run outside the perimeter of the CAA. If classified data is transmitted through a space of lower classification, then a PDS is required. A PDS is required when classified data traverses a hallway of lower classification from one SR to another SR, even if the hallway has some access controls at the lower level. The IA PUB 5239-22 references NSTISSI No. 7003, as a source document for PDS requirements.

81. On 11 March 2011, W6 certified that the physical environment at SSP HQ (Building 200) was mutually classified as both a CAA and RAA. As such, she certified that the environment provided adequate protection for processing classified information, including a physical and electronic constructed access control system. Specifically, W6 certified that the CAA/RAA designations were in compliance with the physical security requirements of SECNAV M-5510.36.

82. On 27 May 2011, Commander Naval Network Warfare Command issued an Interim Authorization to Operate (IATO) SSPs Classified Local Area Network (CLAN) version 4.0 on the classified legacy network. This IATO granted operation of SSP's CLAN at SSP HQ, Program Management Offices, UK Liaison Offices, and Strategic Weapons Facilities.

83. On 19 September 2011, Defense Information Systems Agency issued SSP HQ an Approval to Connect the SIPRNET, which is valid until 31 August 2014.

84. From 23 to 31 January 2013, NAVINSGEN conducted a command inspection of SSP HQ, during which the inspectors spoke to Mr. Edwards. The NAVINSGEN inspection report noted Mr. Edwards had been on board eight months and, during that time, conducted a self-assessment of SSP HQ spaces. Mr. Edwards noted shortfalls in security standards during the command self-assessment and follow-up evaluation to include: 1) gaps in physical and information security; 2) lack of a functioning intrusion monitoring system; 3) lack of solid core doors on spaces designated as secure areas; 4) lack of recordkeeping on security incidents; and 5) a need to draft a new instruction and Emergency Action Plan in order to improve overall security awareness and practices. The NAVINSGEN report verified that there were deficiencies and noted that SSP HQ developed a plan of action to address these issues, including updating instructions, emergency action plans, increased security awareness, and proactive efforts to mitigate security shortfalls. There is no information in the report concerning SIPRNET deficiencies or vulnerabilities. According to W 14 Mr. Edwards raised security concerns which included SIPRNET deficiencies to the NAVINSGEN inspection team. NAVINSGEN did not report the SIPRNET deficiencies in the report, because at the time, SSP was scheduled for a March 2013 CCRI and had an action plan that included an action to address the SIPRNET deficiencies.

85. In an 11 March 2013 e-mail, W 21 , informed W 10 and Mr. Edwards that FCC was scheduled to conduct a CCRI from 25 to 29 March 2013 to assess compliance with SSP's defense information system. However, FCC postponed this CCRI. FCC was formally rescheduled via Naval message 291940Z May 13.

86. Both the complainants and W 17 testified that in preparation for the CCRI, SSP HQ conducted an internal assessment of their compliance of cyber readiness. No timeframe for this internal assessment was identified; however, according to Mr. Edwards' e-mail of 14 March 2013, the internal assessment continued into late March 2013.

87. On 6 February 2013, Mr. Edwards e-mailed W 22 , Cybersecurity Office of the DON CIO, and provided his security concerns about the previous CSM's [W 6] certification of the CAA. As a result, he requested the definition of processing classified information, and noted that he had a problem with 220 SIPRNET ports in SSP HQ's CAA. Mr. Edwards attached a plan of action to address physical security deficiencies, specifically the glass doors.

88. On 6 February 2013, W 22 forwarded Mr. Edwards' 6 February 2013 e-mail with security concerns to W 23 , Certified TEMPEST Technical Authority, SPAWARSYSCEN Pacific, requesting that he review the information provided by Mr. Edwards and provide recommendations.

89. On 6 February 2013, W 23 notified Mr. Edwards via e-mail that if classified data lines leave the CAA or go between CAAs, then a PDS is required. He opined that based on the information Mr. Edwards provided in his 6 February 2013 e-mail that the SSP CAA did not meet the security requirements.

90. W 17 testified that the SIPRNET was not encased in a PDS because all of SSP HQ was a CCA and as a result, PDS was not required. He further testified that he advised Mr. Edwards that if Mr. Edwards decertified spaces, he would have to pull SIPRNET out of those spaces because there was no PDS. W 17 acknowledged in his testimony that once it was determined that the physical security deficiencies in the CAAs were not going to be corrected; he began pulling SIPRNET back from all of the stations outside the CAAs and OSSs. He testified that they removed the terminals, disconnected switches, and pulled the cabling. He explained in his testimony what he meant by "pulling SIPRNET." He testified they pulled the Wyse thin client transceiver and any wires that were connected. They then went into the wiring closet and through the switches, disconnected everybody from SIPRNET who were outside CAA and OSS spaces.

91. On 21 February 2013, SSP HQ notified employees via the 21 February 2013 Official Newsletter that SIPRNET terminals would be removed from SSP HQ offices, conference rooms, and cubicles until SSP HQ remediates vulnerabilities in SSP HQ's CAAs. The Newsletter also stated that SIPRNET processing would be allowed in the Communications Center and room SP205. W 10 testified that SSP began removing unprotected SIPRNET on 1 March 2013 and completed the effort by 20 March 2013. In an e-mail dated 28 July 2014 to IO 1 , NAVINSGEN Investigations Branch Head, W 24 , SSP IG, corroborated that the SSP HQ IT staff began pulling back SIPRNET from unsecure spaces on 1 March 2013 and completed the pull back on 20 March 2013.

92. On 18 March 2013, Mr. Edwards sent an e-mail to W 10 , advising that he had informed the command that the following problems existed: (1) No adequate means to protect SIPRNET as

required; (2) No PDS existed for SIPRNET or lock boxes; (3)SSP HQ did not have a current designated CAA for the SIPRNET lines running throughout the Command and certain areas had active network ports; (4) Room SP205 was not currently designated an OSS or a CAA; (5) there was no kill switch on the SIPRNET; and (6) physical security requirements were ignored even by SSP leadership as SIPRNET is viewed and used with windows up and left logged on when not monitored. In his e-mail, he opined that there should currently be no SIPRNET in the SSP.

93. On 18 March 2013, Mr. Edwards sent an e-mail to W 17 asking if the SIPRNET had been turned off to all SSP HQ spaces and noted that SSP did not have "any" open storage or CAA in the SSP spaces, minus those certified for higher than secret classification. He acknowledged that the previous CSM [W 6] generated letters for CAA and OSS, but clarified that the CAA and OSS certification packets were not complete and those that she did complete, were done on the wrong form. He further stated in his e-mail that he could not certify any SSP spaces as CAAs or OSSs because the command had not yet informed him of a security-in-depth check. There is no record that Mr. Edwards decertified any CAA or OSS spaces, which as CSM would have been his responsibility.

94. On 18 March 2013, W 17 responded to Mr. Edwards' e-mail of 18 March 2013 asking if SIPRNET had been turned off. W 17 informed Mr. Edwards that he was still in the process of removing SIPRNET terminals from the SP30 space and the front office until proper physical security could be established, and further stated that SIPRNET was still operating in the Communications Center and SP205 spaces. He also informed Mr. Edwards that if he, Mr. Edwards, was directing to shut down SIPRNET in the entire command; he would have to take that to the SSP HQ Board of Directors.

95. On 14 January 2014, W 25 , SSP Deputy CIO, testified that the SIPRNET did not have PDS from May 2012 until March 2013, because the certification [CAA] by the previous CSM deemed all cabling in the "perimeter" and there was no need for those devices [PDS or lock boxes]. He further testified that due to ambiguity in physical security, they pulled the SIPRNET, with the exception of OSSs only, making the kill switch no longer a requirement. When asked what knowledge he had of SIPRNET lines being run over unsecure hallways; he confirmed he was aware questions arose about SIPRNET lines running over unsecured hallways.

96. W 10 testified that once SSP discovered that the doors and the other requirements did not meet the security requirements for a CAA, they removed the SIPRNET terminals from the offices in areas that were not OSSs. He acknowledged they removed some 200 SIPRNET terminals. He testified that they removed only so many SIPRNET cables/wiring a day and it took quite a few weeks to disconnect, inventory, and store the many terminals. According to W 10 , removal meant they disassembled and wrapped up the SIPRNET cables and disconnected SIPRNET wiring. He testified they did not shut down the entire SIPRNET but continued to maintain SIPRNET in the approved secure areas, the Communications Center and in Room SP205.

97. On 19 February 2014, W 5 testified that at the time Mr. Edwards left SSP (19 March 2013), one of the security violations that needed to be corrected was with the SIPRNET. He testified that the command made the decision to retrench/turn off SIPRNET access to all but secure spaces until physical parameters could be put in place to properly deploy it SIPRNET to individual desktops.

98. On 16 July 2014, W 19 , testified that because they identified security related deficiencies with the glass doors in the SSP HQ spaces, they pulled the SIPRNET that was outside two certified spaces Communications Center and Room SP205. He testified that they left SIPRNET connected in the certified Secret areas.

99. Defense Information Systems Agency (DISA) conducted a CCRI of SSP from 6 to 10 January 2014. According to the CCRI Compliance Report, DISA found SSP's SIPRNET compliant with applicable directives.

Allegation Four

100. In addition to the findings of this allegation, the findings, analysis and conclusions of Allegations Two and Three are adopted.

101. The complainants in their testimony stated that "while SIPRNET was shut down in some offices, SIPRNET was maintained in other offices."

102. SECNAV M-5510.36, Section 4, states "when conditions exist that prevent compliance with a specific safeguarding standard or costs of compliance exceed available resources, a command may submit a request for a waiver or exception to the requirements

of this policy manual, in writing, via the chain of command to the CNO (N09N2). Each request shall include a complete description of the problem and describe the compensatory procedures, as appropriate. A waiver may be granted to provide temporary relief from a specific requirement pending completion of action which will result in compliance with this policy. An exception may be granted to accommodate a long-term or permanent inability to meet a specific requirement."

103. On 27 January 2012, W 26 , Flag Communicator, stated that he was tasked by W 17 to review SSP's security programs (Information, Industrial, Original Classification Authority, Security Education, Security Letter of Agreement, Memorandum of Agreement, Memorandum of Understanding, North Atlantic Treaty Organization Programs and Security Violations) with members of SSP HQ security staff (W 27 , Security Specialist W 28 , W 29 , W 30 and W 31) in preparation of SSP's June 2012 CCRI.

104. W 17 testimony corroborates W 26 e-mail in that he [W 17] tasked W 26 to assess SSP's physical security posture in preparation for the CCRI since he [W 26] was SSP HQ Communication Center's leading Chief and no one else had the experience.

105. On 18 June, 2012, FCC was scheduled to conduct a CCRI at SSP HQ to assess SSP HQ's compliance of their defense information system. FCC subsequently rescheduled the CCRI to October 2012 citing a schedule conflict for their command.

106. On 1 October 2012, SSP HQ was scheduled to "go-live" and transition to Navy Enterprise Resource Planning (ERP), DON's financial management system of record that standardizes Navy business practices. To eliminate operational conflicts with critical ERP transition timelines and resources and the CCRI occurring simultaneously, W 5 requested that the inspection not take place in October during the transition.

107. The CCRI was scheduled to be conducted a second time on 25 March 2013. However, due to FCC's travel restrictions, the CCRI was rescheduled for the final time for January 2014.

108. In preparation for the CCRI, SSP HQ conducted an internal assessment of their compliance with cyber readiness requirements. During their self-assessment, Mr. Edwards noted security concerns with the SIPRNET (e.g., active and unprotected

lines) and contacted Defense Security Service (DSS) for assistance. Mr. Edwards assessed that the command security's posture was vulnerable.

109. Mr. Edwards contacted, via e-mail, W 32 , Physical Security Specialist, DSS, and W 33 , Chief of Security, DSS and requested that they conduct a courtesy assessment of SSP's security posture.

110. W 32 testified that in February 2013, Mr. Edwards contacted him to assist with the upcoming CCRI as a "set of outside eyes." W 32 further testified that he conducted a courtesy assessment in early 2013 by completing a walk-around of SSP spaces. W 32 stated there was no mention of a concealed or reactivated SIPRNET during his walk-around. W 32 also testified that he did not send a report of this walk-around to SSP.

111. W 33 testified that in early 2013, Mr. Edwards contacted his physical security specialist [W 32] for assistance with SSP HQ's upcoming CCRI and asked for a courtesy walk-around with him of security concerns. Both W 32 and W 33 conducted a courtesy assessment by completing a walk-around of SSP spaces. W 33 also stated that there was no mention of a concealed or reactivated SIPRNET and that W 32 did not send SSP a report of the walk-around.

112. On January 2013, NAVINSGEN conducted a Command Inspection of SSP HQ; the inspectors found no evidence that SSP concealed or reactivated the SIPRNET.

113. On 21 February 2013, the SSP HQ staff was informed via an official newsletter that SIPRNET terminals for access to classified material would be removed from certain offices, conference rooms and individual cubicles until the physical security vulnerabilities associated with the spaces where the SIPRNET was removed were remediated. The SSP HQ newsletter informed the staff that access to SIPRNET would only be available in the Communication Center (COMCEN) and Operations, Evaluations and Training Branch (SP205) from 0700 to 1700.

114. On 11 March 2013, Mr. Edwards provided security requirements via e-mail for W 5 bi-weekly remarks to the staff in preparation for the 25 March 2013 CCRI.

115. On 12 March 2013, FCC contacted SSP and informed W5 that the 25 March 2013 CCRI would be rescheduled for FY14. This was due to travel restrictions placed on FCC.

116. On 13 March 2013, W34 , FCC, Original Classification Authority, e-mailed W5 to followed-up on the verbal discussion regarding the rescheduled inspection.

117. On 14 March 2013, Mr. Edwards sent an e-mail to W32 , and stated that "although SIPRNET access was removed from most spaces in SSP, SIPRNET terminal access remained in W5 office and six other offices (e.g., front office staff)."

118. On 18 March 2013, W17 e-mail stated that "SIPRNET access had not been turned off in all spaces; however, the process to remove SIPRNET access was in progress. All SIPRNET terminal access was completely pulled back by 20 March 2013."

119. W17 testified that the SIPRNET terminals were removed, the switches were disconnected and the SIPR cables were "pulled back." He further testified that the SSP front office SIPRNET access was pulled back. The front office consisted of the Director, the Deputy Director, the Technical Director, and the Director Plans and Programs.

120. On 20 March 2013, SSP HQ established SIPRNET access to the designated SR. Based on W10 testimony, no changes to SIPRNET system distribution and deployment were made since 20 March 2013. Based on the information available with respect to the SIPRNET being pulled back to the secured rooms, SSP was found to be in compliance.

121. FCC postponed SSP's CCRI, that was scheduled for 25 March 2013, and rescheduled the CCRI for 6 to 10 January 2014, citing FCC travel restrictions.

122. W5 testified that "the command decided to retrench the SIPRNET access to the secured spaces until proper deployment could take place."

123. W10 testified that "the SIPRNET lines were not hidden, covered up or reactivated."

124. W10 further testified that "the terminals were disconnected, inventoried and stored."

125. W 19 testified that SIPRNET was "pulled back" to mitigate the unprotected SIPRNET terminals.

126. FCC conducted the CCRI from 6 to 10 January 2014; SSP received an overall grade of 88.0, one of the highest ever attained in the DON which demonstrates an external validation of SSP HQ's security operations and status.

Allegation Five

127. DoDD 8100.02 establishes a general restriction on PEDs in classified areas.

128. DoDD 8100.02, paragraph 2.3, states that this directive "Applies to all commercial wireless devices, services, and technologies, including voice and data capabilities, that operate either as part of a DOD Global Information Grid (GIG), or as part of DOD non-GIG Information Technology (IT) (stand-alone) systems. This includes, but is not limited to: commercial wireless networks and Portable Electronic Devices (PED) such as laptop computers with wireless capability, cellular/Personal Communication Systems (PCS) devices, audio/video recording devices, scanning devices, remote sensors, messaging devices, Personal Digital Assistants (PDA), and any other commercial wireless devices capable of storing, processing, or transmitting information."

129. DoDD 8100.02, paragraph 4.2, states that "Cellular/ Personal Communications Systems (PCS) and/or other Radio Frequency (RF) or Infrared (IR) wireless devices shall not be allowed into an area where classified information is discussed or processed without written approval from the Designated Approving Authority (DAA) in consultation with the Cognizant Security Authority (CSA) Certified TEMPEST Technical Authority (CTTA)."

130. DoDD 8100.02, paragraph 4.3, states that "Wireless technologies/devices used for storing, processing, and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted unless approved by the DAA in consultation with the CSA CTTA. The responsible CTTA shall evaluate the equipment using risk management principles and determine the appropriate minimum separation distances and countermeasures."

131. SSP Instruction (SSPINST) 8100.1 prohibited cellular telephones, including photo-cable cellular telephones, in areas

where classified information is discussed, processed, or electronically stored at SSP HQ during classified discussions and at all times in areas authorized for classified electronic processing. Visitors were not authorized to carry photo-capable cellular phones while in SSP spaces and were required to store them with the SSP Security Office upon check-in. The instruction did not address PEDs other than cellular telephones and had inconsistencies in application. In the opening statements, SSPINST 8100.1 specified all cellular telephones; however, throughout the remaining instruction it was specific to cellular telephones with photographic capability, and specifically the statement of compliance for all employees signature only indicated photographic capable cellular telephones.

132. SSP HQ occupied Building 200 in December 2010. On 3 March 2011, W6 , the CSM, certified Suite SP202, Room 5318 (fifth floor) as an OSS for classified meetings at the level of Top Secret and below, in accordance with SECNAV M-5510.36.

133. On 11 March 2011, W6 also certified that the physical security environment at SSP HQ was mutually classified as both a CAA and RAA. As such, she certified that the environment provided adequate protection for processing classified information, including a physical and electronic constructed access control system. Specifically, W6 certified that the CAA/RAA designations were in compliance with the physical security requirements of SECNAV M-5510.36.

134. On 5 August 2011, W6 certified that Rooms 4103 and 4103A (fourth floor) were inspected and certified to meet the physical standards of SECNAV M-5510.36 and were designated as SRs/CAAs authorized to handle and process classified materials up to the level of Top Secret.

135. From December 2010 to November 2013, SSP permitted personnel to bring cellular telephones and other PEDs into CAAs and use them in these areas when classified information was not being discussed, processed or electronically stored in the area. An SSP employee testified on 3 June 2014 that, "Now we can't have cell phones at our spaces. They have lock boxes now in the security and in the different hallways. We lock them up now." The employee stated prior to the lock boxes being installed, "We all used our cell phones in our areas, because we had an instruction allowing us to have it." The SSP employee testified

that there were some restrictions on cellular phones, "We could not have cellular phones in the Management Center (MC) during classified meetings."

136. Mr. Edwards, one of the complainants, testified that he observed a variety of PEDs, including cellular telephones, within CAAs and OSSs. He also testified that he observed SSP personnel, contractors, and visitors using cellular telephones and other PEDs in CAAs and OSSs, in violation of DoDD 8100.02.

137. W 1 , W 28 , W 17 , and W 18 , a contractor employee at SSP, confirmed through testimony that SSP personnel and others brought cellular telephones and other PEDs into CAAs and OSSs and used them in those spaces. Mr. Londagin, one of the complainants, stated SSP installed a tower or a dish on the roof of Building 200 that improved the strength of the cellular signal. Mr. Londagin stated depending on the direction the tower or dish was pointed, the signal strength improved for some wireless network providers, such as AT&T, Verizon and Sprint. At the time, DoD and SSP policy allowed PEDs in CAAs when not processing classified information.

138. Mr. Edwards testified that "intensifiers" or "repeaters" were installed in OSSs around December 2012 or January 2013, to improve the strength of the cellular signal, in violation of DoDD 8100.02. Mr. Edwards testified, "We blocked Yahoo on the internet, so they had to get on their cell phones at their desk to check their Yahoo accounts. Instead of taking cell phones out, we intensified certain provider signals because people weren't getting good reception in their offices."

139. W 18 testified that SSP had a project to install intensifiers in rooms to intensify the cell signal. On 5 June 2014, W 18 stated that SSP personnel can no longer have cellular phones in SSP HQ spaces, but they had previously been allowed to have cellular phones, and the intensifiers provided for reception.

140. Mr. Edwards testified that in May 2012, during his initial walk-through of SSP HQ with W 10 they entered into an OSS and "there was a bookshelf inside the space and everybody's phones are in it." Mr. Edwards stated that W 10 told him, "This is where everybody puts their phones." Mr. Edwards testified, "I said, why is this in the space? This is open storage secret. It's wide open. Everybody's iPads, their

personal laptops, their cameras, their phones, they're all sitting there, they're sitting there using them."

141. Mr. Edwards testified, "I requested boxes to be installed outside the door (OSS) to move them outside the area, immediately put them outside. I got that part. The rest of the space they said, draft a PED policy. I drafted it and it waited for signatures forever, they really never took action." Mr. Edwards did not provide a date for this draft, nor was the draft located. Mr. Edwards said he told them that in the interim, the devices have to be outside or they would fail the Cyber Command Inspection. Mr. Edwards testified, "DSS told them. The IG Inspector said the same thing." To address Mr. Edwards' concerns there were two lock box units ordered on 4 May 2012, and they were installed in June 2012. There were additional lock boxes installed 25-26 June 2013. Prior to the lock boxes being installed, Mr. Edwards testified that there was a bookshelf inside OSS, where cell phones were stored.

142. SSPINST 5230.14, Commercial Mobile and Wireless Device, Service, and Technology Policy, of 19 November 2013, replaced SSPINST 8100.1 and established new policy and procedures for Commercial Mobile Devices (CMDs). SSPINST 5230.14 prohibits PEDs in SSP CAAs and SRs due to the increased risks of information compromise through use of new technology, but states CMDs can still be used in RAAs and Limited Access Areas (LAAs). SSPINST 5230.14 also authorizes Government-owned and issued CMDs in SSP CAAs, but they must be physically removed when classified information is being electronically stored, processed, transmitted, or discussed. SSPINST 8100.1 prohibited cellular telephones, including photo-cable cellular telephones, in all areas where classified information was discussed, processed, or electronically stored; while SSPINST 5203.14 only limits prohibitions to CAA and above.

143. On 1 March 2013, Mr. Edwards reported a Security Violation (SECVIO) 03012013-008 that involved "camera phones, digital cameras and large telescopic cameras being allowed in the MC," which is a CAA, during a ceremony. The report stated the Security Manager reminded SSP leadership that cellular phones were prohibited in the MC and all visitors were instructed to leave their cameras in the Security Management office upon check-in. In passing by the MC during the ceremony, Mr. Edwards noted that approximately five cameras were visible and in plain view.

144. The SECVIO 03012013-008 report stated security measures were purposely defeated, and SSP leadership asked the CSM to perform an unethical function/practice by "turning a blind eye." Mr. Edwards provided a statement regarding the incident that read: "I received a call from W9 via my office phone during the ceremony or just shorty after it ended. W9 informed me that the command's stance on ceremonies was to turn a blind eye to this in the MC. He went on to say, I am asking you to turn a blind eye for these events."

145. In late August 2013, W19 was given a package of issues and allegations that Mr. Edwards provided on 19 March 2013. In a 5 September 2013 Memorandum for the Record addressing Mr. Edwards' allegation that W9 told him to "turn a blind eye," to cameras in the MC, W19 wrote "There was not written documentation or means to substantiate claim and essentially, it came down to being one person's word against another."

Allegation Six

146. SECNAV M-5510.36, Section 10-12, states that "safe combinations will be changed when first placed in use; when an individual knowing the combination no longer requires access unless other sufficient controls exist to prevent access to the lock; when subjected to compromise; or when taken out of service. Combination padlocks will be reset to the standard. Personnel who have the responsibility and possess the appropriate security clearance eligibility and access will change combinations to security containers, vaults and secure rooms." Section 7-11 of the manual states "END-OF-DAY SECURITY CHECKS Commanding officers shall establish procedures for end of the day security checks, utilizing the SF-701, Activity Security Checklist, to ensure that all areas which process classified information are properly secured. Additionally, an SF-702, Security Container Check Sheet, shall be utilized to record that classified vaults, secure rooms, strong rooms and security containers have been properly secured at the end of the day. The SF-701 and SF-702 forms shall also be annotated to reflect after hours, weekend and holiday activities. These forms may be destroyed 30 days after the last entry unless they are used to support an ongoing investigation required by Chapter 12.[46]

[46] Per the SECNAV M 5210.1 of November 2007, the retention of the SF701/2s was reduced to one day following last entry. The one-day retention rule is the current controlling guidance, it supersedes the older 30 day retention rule.

147. The allegation is most easily analyzed by dividing it into two parts; first, an examination of the "inspection" requirement and second, the requirement to change safe combinations, upon certain eventualities.

148. SSP HQ maintains roughly 186 safes certified to hold classified documents. In accordance with SECNAV M-5510.36, those safes are required to be checked (inspected) daily (work days) to ensure that they are properly secured. SSP HQ personnel using the safes are responsible for conducting the end of the day review of spaces and safes. In their review they use the SF-702 to document the daily "check." The form is customarily attached to the safe. The SF-701 is used to annotate a similar required daily check of classified spaces, i.e., the SF-701 is used for rooms and the SF-702 is used for safes.

149. During the NAVINSGEN Command Inspection of SSP in January 2013, NAVINSGEN reviewed SSP compliance with the Manual's requirement for daily safe checks and found one SF-702 that was not properly completed. At that time, the complainant, who was accompanying the NAVINSGEN personnel, informed the Inspector that failure to consistently fill-out SF-702s was a continuing problem at SSP HQ; but that it was being addressed by the chain of command. Testimony collected during the SSP investigation indicated that the required checks were being performed.

150. SECNAV M-5510.36, Section 10-12, lists the necessary conditions that prompt a required combination change. Documentary evidence, in the form of e-mails, from various Codes throughout SSP, to the CSM, shows that safe combinations were being changed but the evidence was insufficient to determine the reason(s) those changes were made. When a combination is changed it is recorded on an SF-700. All SF-700s were compared against the SSP Alpha Roster. Six individuals, with access to a safe, were identified as having left SSP and the combination of the corresponding safe was not changed. Those six employees all left after the period identified in the allegation.

151. W 10 testified that the complainants are responsible for changing safe combinations. Mr. Edwards is delegated this responsibility through an appointment letter designating him as the CSM. The appointment letter references the SSP Security Manual, which assigns the CSM specific responsibilities, including changing safe combinations. W 10 further testified that the complainants never reported to him that they were having difficulty in making combination changes due to

resistance from individual employees or SSP leadership (as the complainants' assert in their testimony).

152. Internal SSP rules require all departing personnel to visit the Security Office for a departure clearance (CHECKOUT FORM). As a part of this process, departing personnel are required to turn in security badges and listen to a 30-minute brief. This checkout process with Security, alerts the CSM to change the combination of any safe to which the departing employee has access. The complainants, in their testimony, make it clear that they were unable to fully perform their duty to make necessary combination changes because of SSP resistance.

Allegation Seven

153. This allegation will be discussed in two parts. The first part will examine the positioning of computer screens within SSP HQ spaces, such that classified information may have been visible to individuals without appropriate clearances. The second part will address the issue of unattended CACs.

154. SECNAV M-5510.36, Exhibit 10A, states that "All windows that might reasonably afford visual observation of classified activities within the facility shall be made opaque or equipped with blinds, drapes or other coverings" and Section 7-10 states that "...classified material may not be opened or read in any area where it can be seen by unauthorized individuals."

155. The SSP FDC, MILCON Project P-402C requires blinds be provided for all SSP windows in Building 200. The NAVINSGEN Command Inspection of SSP in January of 2013 found all windows had appropriate blinds in place. The complainants' testimonial assertion appears to be that the blinds were not used, that they (the Security Department) have to constantly remind people to put the blinds down and that they met resistance from individual employees and SSP leadership in complying with their demand to lower the blinds.

156. Computer monitors are not secured to tables/desks and can be repositioned by the user. The testimony of several witnesses confirmed that there have been occasions when computer monitors were observed facing windows and had to be repositioned. Only one person testified that they specifically observed a SIPRNET computer monitor, which was on, facing a clear window. The blinds, at that time, were two thirds (2/3) of the way down the window.

157. In their interview, the complainants alleged that they observed, from buildings surrounding Building 200, SSP HQ SIPRNET computers that were turned on and visible to unauthorized individuals. Mr. Edwards specifically alleged that he saw W5 SIPR monitor from across the street while standing in the parking garage.

158. W5 Flag Lieutenant (LT) was questioned over Mr. Edwards' assertion regarding the Admiral's computer monitor. The Flag LT testified that he had been in that, or similar, positions with the Admiral for 3 ½ years; throughout the time the complainants worked at SSP HQ. He provided a description of the Admiral's office and the location of the computer monitor, which was in a hutch with 1 to 2 foot sides, positioned behind the Admiral's desk, perpendicular to the windows facing the parking garage. The Admiral's computer was capable of communicating on both the classified (SIPRNET) and unclassified (NIPRNET) network. A toggle switch enabled the Admiral to go from one network to the other. The Flag LT testified he did not think it would be feasible for anyone to have seen the Admiral's monitor from the parking garage given the distance between them and the location of the monitor in the hutch. He also testified that he never heard of this allegation before being interviewed (25 July 2014).

159. No testimony was obtained nor was any documentary evidence found to support the complainants' general testimonial allegation that SIPRNET monitors were visible through windows from surrounding buildings.

160. DODI 1000.13, Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals. Enclosure 3. Procedures, Section 2. Guidelines and Restrictions, paragraph h: an ID card shall be in the personal custody of the individual to whom it was issued at all times. Full time possession of CACs by Navy personnel is also mandated by DON CIO Msg Dtd 031648Z Oct 11, Para 5.G.(4), which requires all Navy personnel to "Protect Authentication tokens (E.G. Common Access Card) ... at all times ...shall not be left unattended....

161. CACs are issued to DoD personnel for personal identification purposes and for use in accessing unclassified computer systems. SSP HQ SIPRNET remote terminals do not use a CAC for logon purposes. During the time the complainants worked at SSP HQ SIPRNET computers were accessed by means of user

name/passwords; after they left the command, SSP HQ transitioned to tokens in order to log onto SIPRNET.

162. Several witnesses confirmed that CACs were periodically left unattended; this was also observed during the NAVINSGEN Command Inspection of SSP. The CSM's supervisor acknowledged the problem and stated the organization was trying to correct it. If the CSM found unattended CACs, he would take them to the Security Office and the employee would have to go there to retrieve it.

Allegation Eight

163. DODI 5200.08, paragraph 3.4, state:

> Commanders at all levels have the responsibility and authority to enforce appropriate security measures to ensure the protection of DoD property and personnel assigned, attached, or subject to their control.

164. SECNAV M-5239.1, paragraph 2.4.11, states:

> Leadership support at all levels is the most important part of a command's IA program. In their role as local IA authorities Commanding Officers/Officers-in-Charge (COs/OICs) are directly responsible for identifying vulnerabilities in their operational environments and implementing the appropriate countermeasures. COs/OICs are responsible for ensuring that personnel under their command are trained and abide by IA policy. Commanders of DON organizations shall ensure that all IT assets they oversee and operate are accredited and operated in accordance with the accreditation documentation.

165. SECNAV M-5510.36 requires DON commanding officers to manage their command's Information Security Program (ISP) in compliance with that manual. The manual specifies what safeguards are required for classified material handling and storage. Regarding the basic requirement for the proper storage of classified materials, the manual specifically states in Chapter 10 that:

> Commanding officers shall ensure that all classified information is stored in a manner that will deter or detect access by unauthorized persons. Classified information that is not being used or that is not under the personal observation of cleared persons who

> are authorized access shall be stored per this chapter. To the extent possible, limit areas in which classified information is stored and reduce current holdings to the minimum required for mission accomplishment.

166. In May 2010, then W5 assumed command as DIRSSP.

167. As previously noted, Mr. Edwards was the SSP CSM from May 2012 to March 2013. He was preceded in that position by W6 . She left her position with SSP and retired from Federal service in December 2011, approximately six months before Mr. Edwards was hired.

168. There was inconclusive testimony about who may have been the "acting" CSM during the period of time between W6 retirement in December 2011 and the hiring of Mr. Edwards in May 2012. W10 testified that he believed that it was "probably" W7 , who was at the time the Branch Head over W6 and W10 . W10 testified that W7 may have performed the duties of the CSM, however, he stated that he did not "really know if there was ever an official letter designating anybody during that time."

169. W6 was the SSP CSM when SSP occupied office spaces located in Crystal City and during the time that Building 200 was being remodeled. As the CSM, she was responsible for certifying and accepting SSP spaces for compliance with physical security and information security requirements.

170. SSP HQ relocated from Crystal City to Building 200 on the WNY in December 2010. After SSP HQ relocated to Building 200, W6 identified problems with the operation of the ACS that was installed during the renovation project. On 13 January 2011, she reported the problems she had become aware of to W35 , a NAVFAC employee, who served as the Building 200 Construction Project Manager and oversaw the building's renovations from 2008 to 2010. W6 wrote in an e-mail to W35 on 13 January 2011 that all alarm and access control systems were off-line for the SSP HQ spaces on the second and fourth floors in Building 200.

171. W10 testified at length about the faulty ACS that had been installed in Building 200, before occupancy, and the trouble that SSP HQ experienced with the alarm system in the

months following SSP HQ's move into Building 200. W 10 stated:

> We started finding as we moved in here that we were getting alarms showing up and we have a monitoring system here that we would monitor and you'd see alarms coming up [and the system would identify the alarm source] it's this door, let's say, and we would go check and that door's really not -- there's nothing wrong with it. It's not unlocked. It's not open. The base also monitors that and the base was sending over the policemen and, you know, the security guards all the time to -- check them out. So we got -- we contacted the installer, the people who installed the security system. It's a Lenel [ACS] security system. It's the same one the majority -- a lot of -- a number of the organizations on the base use. So it all ties into the same system.
>
> We met with NAVFAC. We met with Naval Support Activity Washington folks who monitor the alarm systems, [and tried] to get them to figure out why this was happening. We got with the -- Convergent, which was the company who installed it, and they were a subcontractor to the building renovation effort, to try and figure what was going on. The base started -- I believe they were -- they started masking the alarms during working hours.
>
> . . .
>
> We would still get them every day. We would get them and we would go through them and check them out. So we weren't ignoring them at all. It was the base during working hours. Now, they would not ignore any of our secure areas, the open storage areas. [If an] alarm came over, they were over here in a minute. If it was an [alarm for a sensor] they hadn't seen before, they would call us.

172. Despite the malfunctioning ACS, on 11 March 2011, W 6 certified that the spaces SSP HQ occupied in Building 200 met physical security requirements of SECNAV M-5510.36. She also specifically certified that SSP HQ spaces were mutually classified as both a CAA and RAA. As such, she erroneously certified that SSP HQ spaces provided adequate protection for processing classified information and that

appropriate access controls were in place. Based on other discrepancies with physical security identified throughout the report, her certification of CAA spaces was defective from the start.

173. Around the same time that W6 made her certification, W7 W6 supervisor, received information that the access control procedures at the WNY were lacking. Although we were unable to obtain a copy of W7 22 February 2011 e-mail, we know she shared this security vulnerability information with SSP HQ staff, to include the Strategic Programs Royal Navy Branch (SP50). The SP50 offices were located in Building 200.

174. On 23 March 2011, W8 sent a letter to W9 ssing concern about the security vulnerability information W7 had reported in her 22 February 2011 e-mail about WNY gate access control procedures. In his letter to W9 W8 wrote:

Official Sensitive PSA

[redacted]

Official Sensitive PSA

[redacted]

175. W8 requested W9 inform him what steps would be taken to bring the level of security at Building 200 up to the standards that were in place when SSP HQ occupied office spaces in Crystal City. In response to W8 request, W9 directed a meeting for concerned parties, which was held on 5 April 2011 and attended by SP50 and SSP Security Department personnel. During the meeting, SP50 explained the process required for developing their (UK) security rating posture and what was necessary to achieve an acceptable security rating. Thereafter, on 25 April 2011, a summary of the meeting and the SP50 security requirements were reported back to W9 .

176. On 20 July 2011, W9 e-mailed W11 , Naval District Washington about the physical security and WNY access control issues that had been reported to him. W9 copied W5 , W12 W13 W10 and W6 on his e-mail and wrote:

Official Sensitive PSA

[redacted]

Official Sensitive PSA

[redacted]

177. The foregoing finding can affect the security situation in Building 200 for all tenant commands with classified information holdings in their respective Building 200 office spaces, not just the UK contingent. For example, proper protection of classified information for certain spaces (OSSs) relied upon a layered defense as described in SECNAV M-5510.36. In this case, the WNY base entry access control points had been assessed to be inadequate to prevent unauthorized entry into Building 200. At the time and until June 2013, Building 200 did not have guards or any other measures to control entry into the building. It was reasonable to believe, therefore, that anyone gaining access to the WNY could also enter Building 200 undeterred and attempt to gain entry at the door to any of the spaces containing classified information located in the building. Based on W 9 e-mail, this situation did not meet UK information security standards for the protection of classified information.

178. On 1 September 2011, W 9 e-mailed W 11 again to follow-up on his 20 July 2011 e-mail that requested a meeting with the NDW Director of Security, W 36 , and appropriate other NDW and WNY officials to discuss the ongoing security shortfalls identified about access to the WNY and in particular Building 200. W 9 repeated his prior request for "a meeting with all WNY stakeholders" to review SSP's planned changes to security procedures at Building 200. He copied W 5 , W 12 , W 13 , W 10 and W 6 on his e-mail. Throughout the intervening months, W 9 and W 10 continued to engage with officials at NDW and NAVFAC Washington to arrange for security guards at Building 200. Their efforts eventually resulted in a contract being awarded for security guards to control access into Building 200. However, security guards were not in place until June 2013 and procedures for 100 percent ID check of anyone seeking access to Building 200 were not established until September 2013. The delay in achieving 100 percent ID check was because SSP as one of several tenants in Building 200 had to coordinate with the other tenants about the procedures they planned to put into place. W 24 , SSP IG, explained as follows:

> During the initial phasing in of the guard services in June 2013 it was decided to gradually acclimate SSP and the tenants of Bldg 200 to the new guard force requirement. In July 2013 NAVFAC (W 37 , COTR) asked SSP to provide Post Orders and modify the Scope of Work for the new guard services. Post Orders had to be developed in concert with the other tenants of Bldg 200, by acknowledging and incorporating the different requirements of their specific missions. Some of the topics that had to be worked out were hours of operation, visitors, tenants POC's, authorized ID cards, and access doors to name a few. Once all the factors of the Scope of Work and Post Orders were worked out with SSP, NAVFAC and the tenants the 100% ID check was implemented for Bldg 200 in September 2013.

179. Mr. Edwards testified that he personally identified the same vulnerabilities about the WNY access control checkpoints after he took over as SSP CSM; the vulnerabilities that W 7 identified and reported to SSP HQ staff on 22 February 2011. In addition to notifying W 9 about his own security vulnerability assessment of inadequate access control onto the WNY, Mr. Edwards testified that he also notified the WNY Visitor Control Center, the WNY Police, and WNY Commanding Officer, W 38 .

180. Based on the documentary evidence we reviewed and Mr. Edwards' testimony, it was clear that Mr. Edwards began identifying security problems and reporting them to his chain of command starting in June 2012. As an example, on 6 June 2012, Mr. Edwards sent an e-mail to W 10 , copied W 7 and several others and stated:

> I want to address a couple [of] things that came from my meeting earlier. The SSP has all of its spaces at the CAA standing. The problem with this is that there is a massive shortfall in some major areas.

181. Mr. Edwards continued his e-mail listing the various shortfalls that he had noted and listed:

a. Glass doors not meeting the IA Pub 5239-22.4.2 standard;
b. Clear vice opaque windows in spaces that contained or where classified information was viewed;
c. IDS not monitored;

d. X09 door locks were not installed as required for a building that was unguarded;
e. Improper door hinges; and
f. Double doors missing astragals.

182. On 16 October 2012, W9 emailed Mr. Edwards about the command security news letter Mr. Edwards prepared and forwarded to W9 for his consideration and comment. The proposed newsletter for SSP staff spoke to ongoing efforts by the CSM to increase security conditions in Building 200. In his email reply to Mr. Edwards, W9 wrote:

> I have made a few edits to your Security Newsletter (see 1st attachmentshows track changes, 2nd attachment is clean version). Please review tomake sure I did not change the context of your letter and if you are OK withthe changes, W20 will issue as an all hands email with the textfrom the clean version.
>
> Also note that I added "core" hours. Since the base opens the main gates at0530, people begin the normal day at that time, so I made that the startdate. I thought 1800 in the evening was reasonable. So people will need toscan in the front door between 1801 in the evening and 0529 in the morning. I think that is fair. Please confirm that the message is OK so that we can send out. Thanks
>
> Also this is a good way to get the message out. We have buy-in from the BOD and SPOO as W19 and I pre-socialized this message. So we are all behind the improvements you are making. Again I just want to stress it all about how we deliver the message which make a huge difference on how the message is received.

183. On 20 October 2012, Mr. Edwards emailed several SSP officials about security violations that he noted they were responsible for. Mr. Edwards explained in his email to these individuals that they had not properly protected FOUO, PII, UCNI and/or Restricted SSP documents as required by the command security instruction. W9 was copied on Mr. Edwards 20 October email and in reply to it, on 22 October 2012, W9 wrote to Mr. Edwards and W10 and copied the SSP Chief of Staff, CAPT Benton stating:

> Sparky/Bill,
>
> While everything that you are doing regarding security is the "right thing" to be doing, I again want to emphasis that it is all about message delivery where people perceive that they were unaware of the rules (because they were overlooked for so long) and feel blind-sided. So when delivered in a "gotch-ya" environment it is not received as well as when we roll out "expectations" first, then come behind with recommended improvements by doing test walk around with the Branch deputy and Branch Security officers. Then after all understand expectation, we can purposely call them out for violations.
>
> So here is the plan, I am directing that you develop a security all hands presentation to be rolled out at the next senior leadership so we can get feedback and a feel for how it will be perceived. Then refine it to be rolled out to all hands. The presentation should include what we believe are best practice expectations, what should your work space look like when you depart for the day. How should material be protected, covered, etc. What should the branch security officers be looking for and how should branch security duty be performed? What are the responsibilities of the branch security officer of the day when he signs off that a space is free and clear of classified or protected material?
>
> Bottom line is we need to make sure they understand the rules first, then we can begin to enforce them.

184. NAVINSGEN inspected SSP from 23 to 31 January 2013 as part of NAVINSGEN's periodic requirement to inspect all U.S. Navy Echelon II commands. During this inspection, the NAVINSGEN team noted that the Security Manager, Mr. Edwards, had compiled a comprehensive list of security deficiencies and proposed corrective actions. Commenting in the executive summary of the 12 June 2013 SSP command inspection report, the Inspector General stated in the Administrative Program Compliance and Oversight section of the summary that NAVINSGEN inspectors found the SSP security program missing key elements and not compliant with governing instructions. Specifically, the summary stated:

> The SSP Command Security program instruction and the Emergency Action Plan are not current or in accordance

> with DON regulations. Many aspects of the signed security instruction do not apply to SSP's current facilities. SSP has progressed with resolving many of the security concerns revealed during SSP's self-assessment. The command security instruction and Emergency Action Plan are in draft form, being revised to comply with current security directives. NAVINSGEN recognized SSP's ability to self-assess and proactively take steps to improve security practices. A current, revised command security program instruction will solidify the security foundation to ensure the command adheres to the governing security policies, instructions, and directives.

185. In preparation for an expected, but later postponed, CCRI, SSP HQ went about addressing discrepancies. For example, on 21 February 2013, page 1 of the SSP command newsletter included the following announcement related to SSP HQ's ongoing efforts to correct its SIPRNET discrepancies:

> SPHQ SIPRNET Operations
> Several changes are being made to increase the security of SSP networks:
>
> Commencing 1 March - With the exception of the COMCEN (Room 4103) and SP205 (Room 4200), SIPRNET terminals will be removed from SPI IQ offices, Conference Rooms, and cubicles until SPHQ remediates CAT I vulnerabilities in SSP's Controlled Access Area (CAA). In the interim, SIPRNET processing will only be allowed in the COMCEN and SP205 from 0700-1700. For Emergency (Infrequent) access to the COMCEN outside of these hours, please contact the SPHQ Command Duty Officer (CDO) at (571) 481-7438. For Emergency (Infrequent) access to SP205 outside of these hours, please contact the SP205 Duty Officer (DO) at (571) 481-7446.
>
> For Branches that require FREQUENT access to the COMCEN or SP205 outside of these hours, have the Branch Head contact and provide W 26 with a list of the required personnel via the MIS [Management Information System] Help Desk at (202) 433-8777.

186. On 1 March 2013, Mr. Edwards wrote an email to W 9 and requested that Mr. Kethcum review a draft security-in-depth

(SID) determination document Mr. Edwards prepared for W 20 signature. The document requested W 5 determination of SID in order to designate certain SSP assigned space in Building 200 as an OSS.

187. During their clarification interview, the complainants testified and provided additional information about the security concerns they reported up their SSP chain of command; the same concerns they raised in their complaint to the OSC. In particular, the complainants stated they reported that Building 200 was vulnerable because there were insufficient measures to prevent unauthorized access. The complainants noted in particular that the concept of security-in-depth was specifically lacking for the SSP HQ spaces located in Building 200. Both complainants testified that they reported their concerns about security-in-depth to W 9

188. During the time in question, NDW granted access onto the WNY to anyone with a valid State or Federal ID. Also during this time, Building 200 did not have security guards posted; consequently, anyone who gained access to the WNY could enter the building's common areas 24/7 without being challenged or their purpose for entering Building 200 determined.

189. W 9 was interviewed on 16 January 2014 and he testified about his knowledge of the physical and information security concerns that Mr. Edwards reported to him. About those reports, W 9 said:

> Mr. Edwards and I had a conversation regarding deficiencies he found during his reviews. I formally asked that he provide a list [from which SSP could take] corrective actions to bring our security standards in alignment with what he thought were the standards at the time.
>
> . . .
>
> [Mr. Edwards] stated these were requirements but no documents were provided. You can say that something was wrong but you have to show the requirements so I can understand it because I was trying to distinguish between [Mr. Edwards' expectation] and a requirement. Finally, no, he did not bring any violations to my attention.

190. Although Mr. Edwards testified that he had regular communication and meetings with W9 and the SSP Deputy, W20 , about security matters, he also testified that he did not meet directly with W5 to present his concerns about security-in-depth. Mr. Edwards, however, testified that he instead handed W5 a package of information that explained the various security issues.

191. W5 was interviewed on 19 February 2014. He testified as summarized below about the list of security deficiencies Mr. Edwards said he handed to W5 .

> I do remember a list generated of deficiencies; I do not remember [Mr. Edwards] handing me directly any files on potential security violations [on 19 March 2013]. I considered the list appropriate in the sense that [Mr. Edwards] was the head of security and his job to identify deficiencies. I do remember [discussing the list of deficiencies with my] Board of Directors (BOD) and they ... put together a POAM to address [the deficiencies] to ensure they were properly adjudicated….

192. It is unclear whether W5 received the package of information directly from Mr. Edwards. Nevertheless, W5 was in receipt of the information.

193. On 4 August 2014, NAVINSGEN requested that SSP provide BOD minutes dating back to June 2011 but more importantly explain SSP's practice for briefing W5 about BOD results and actions directed. We specifically asked to know when SIPRNET issues (i.e., problems with SIPRNET in CAAs) were first raised to the BOD. W9 responded in an e-mail to the Deputy Naval Inspector General on 4 August 2014. He wrote in part:

> A meeting to discuss [any security matter like SIPRNET] would have occurred at an impromptu BOD meeting and decision minutes would not have been collected.
>
> . . .
>
> Generally all decisions regarding operations, personnel and fiscal matters are made by the 4 member BOD. When a consensus cannot be reached by the 4 member BOD, then the Director SSP is brought into the process for final adjudication. The BOD informally

> briefs the Director of significant matters during the Director's morning or evening daily drive by time.
>
> In January 2013, the SSP BOD was briefed for the first time by the SSP CIO and SSP security manager (Mr. Edwards) regarding potential security issues with the CAA and impacts on SIPRNET. The briefing recommended several options to address potential security issues. In early February 2013 the SSP BOD determined the pull back of SIPRNET to only [SSP HQ] OSS spaces. The Director was not informed of this matter until a decision was made by the BOD to pull back SIPRNET terminals, including the Director's terminal, sometime in early February 2013.

194. W5 recalled that two of the deficiencies in particular stood out among the rest; they were the SIPRNET cabling issue and the glass doors associated with spaces where classified material was stored or viewed. About these two issues he testified:

> The command made the decision to retrench SIPRNET access to the secure spaces in SP16 until physical parameters could be put in place to properly deploy it to the desktop.
>
> [The glass doors were] personally and professionally disturbing since the building was accepted from NAVFAC and it was a fairly sizable resource dollar value that we had to come up with [in order to replace them with compliant solid core doors.] Since this building is a NAVFAC/CNIC building and not under our cognizance, we had to do the funding and or coordination transfer either to NAVFAC or to CNIC. That's work in progress, we will get into the standards but I did not have the authority to instantaneously and solely direct as Director of Strategic Systems Programs. I was the Director of Strategic Systems Programs [when our offices were located] in Crystal City.

195. In his closing comments for the record, W5 testified:

> The information I want to be a part of the record is contained in my last statement is that we hired Mr. Edwards and Mr. Londagin to be the head of security and deputy security to do exactly what they

did which is identify deficiencies. Having done that and presented that as part of what I consider their billet description this program has worked diligently to address those issues. Fortunately or unfortunately, the structure that I've had to work within does not afford me with unilateral authority or sole authority so I've had to work within the constraints, financially and administratively, as the Director, SSP.

We created a POAM, worked through the POAM, and I think our believed perfect score on the Cyber Inspections on physical security reinforces that we take security seriously and our line of business require that we do so. I think they did what they were hired to do which was to point out deficiencies. This program has done what it is accountable to do which is to ensure that those deficiencies are being addressed.

With regard to [Mr. Edwards' and Mr. Londagin's unofficial and independent actions to evaluate WNY entry access controls, which were] outside of [their job] description…. At no time were [their plans to make such an evaluation] discussed with me. At no time were [they] approved by me and at no time [was their doing so] in my opinion appropriate. They were certainly outside the scope of [their] authority. Not within my authority to or theirs to execute actions outside scope [of their authority to] include surveillance of the Navy Yard, and testing the security guards. That is not within the authority I possess. I was not informed of any potential shooters. They [Edwards and Londagin] made comments how they felt but never presented any evidence because if so my comment would have been by whose authority are you doing that because it would not have been mine. I was [not] aware that they entered [WNY] gates with others ID [while conducting their own] investigation.

. . .

If I would have known through direct conversations with them or through any other means I would have stopped that because it is not within my authority or theirs to go execute.

APPENDIX B – DEFINITIONS

Access Control – A system that controls the ability of people or vehicles to enter a protected area by means of visual, manual, or electronic (or a combination of three) authentication and authorization at entry points, and manages identity information for controlling physical access to eligible, authorized persons.

Astragals - a convex molding or wooden strip across a surface or separating panels, typically semicircular in cross-section.

Common Access Card - The common access card (CAC), a form of DoD ID card, shall serve as the Federal Personal Identity Verification (PIV) card for DoD implementation of Homeland Security Presidential Directive 12.

Classified Information – any matter, document, product, or substance on or in which classified information is recorded or embodied, including that classified information that resides on classified Information Technology (IT) systems.

Controlled Access Area - a physical area (e.g., building, room, etc.) which is under physical control and to which only personnel cleared to the level of the information being processed are authorized unrestricted access. All other individuals are either escorted by authorized personnel or are under continuous surveillance. A CAA shall comply with the CAA physical security requirements. Within a CAA, a PDS will not be required for classified information processed at or below the classification level to which access to the CAA is controlled. While unprotected cables may run within the CAA, they will not run outside the perimeter of the CAA. A PDS or CLAN drop is allowed to originate and terminate in a CAA Safeguarding and storage of magnetic and hard copy media is required.

Intrusion Detection Systems - devices that initiate alarm signals by sensing a stimulus, change, or specific condition.

Kill Switch – a mechanism used to shut down or disable machinery or a device or program. The purpose of a kill switch is usually either to prevent theft of a machine or data or as a means of shutting down machinery in an emergency.

Level One - The least secure type of restricted area. It shall be established to provide an increased level of security over that afforded elsewhere aboard the activity to protect a security interest that, if lost, stolen, compromised, or

sabotaged, would cause damage to the command mission or impact upon the tactical capability of the United States. It may also serve as a buffer zone for Level Three and Level Two restricted areas, thus providing administrative control, safety, and protection against sabotage, disruption, or potentially threatening acts. Uncontrolled movement within it may or may not permit access to a security interest or asset.

Level Two - Restricted area may be inside a Level One area but shall not be inside a Level Three area. It shall be established to provide the degree of security necessary to protect against uncontrolled entry into, or unescorted movement within, an area that could permit access to a security interest that, if lost, stolen, compromised, or sabotaged, would cause damage to the command mission or harm the operational capability of the United States. Uncontrolled or unescorted movement could permit access to the security interest.

Level Three - The most secure type of restricted area, it may be within less secure types of restricted areas and shall be established to provide a degree of security where access into the restricted area constitutes, or is considered to constitute, actual access to a security interest that, if lost, stolen, compromised or sabotaged, would cause grave harm to the command mission or strategic capability of the United States. Access to the Level Three restricted area shall constitute actual access to the security interest or asset.

Lock Box - any computerized devices intended to prevent the unauthorized distribution or copying of digitally stored or transmitted data.

Physical Security – that part of security concerned with active and passive measures designed to prevent unauthorized access to personnel, equipment, installations, and information, and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity. It is designed for prevention and provides the means to counter threats when preventive measures are ignored or bypassed.

Portable Electronic Device (PED) - Any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. This definition includes, but is not limited to PDAs, cellular/PCS phones, two-way pagers, e-mail devices, audio/video recording devices, and hand-held/laptop computers.

Protective Distribution System - provides guidance for the protection of wire line and optical fiber cables transmitting unencrypted classified National Security Information.

Pull Box - a metal box with a blank cover that is installed in an accessible place in a run of conduit to facilitate the pulling in of wires or cables

Purge - rendering sanitized data unrecoverable by laboratory attack methods.

Restricted Access Area - a physical area (e.g., building, room, etc.) that is under physical control and to which only personnel cleared to the level of the information being processed are authorized unrestricted access. Authorized personnel escort all other individuals. A Restricted Access Area (RAA) shall comply with the RAA physical security requirements. Safeguarding and storage of magnetic and hard copy media is required. Within an RAA, a PDS is required. A PDS or Classified Local Area Network (CLAN) drop is not allowed to terminate within an RAA unless placed in an approved lockbox with an approved PDS lock.

Secure Room - a physical area which meets the construction requirements for "open storage" at the classification level of the information being processed. A Protected Distribution System is not required for classified information processed at or below the authorized "open storage" level for the Secret Room.

Security-In-Depth - a determination by the commanding officer that a command's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the command. Examples include perimeter fences, employee and visitor access controls, use of IDSs, random guard patrols during non-working hours, closed circuit video monitoring, and other safeguards that reduce the vulnerability of unalarmed storage areas and security storage cabinets.

Secret Internet Protocol Router Network Token - A smart card or *hardware token*, used on the Secret Internet Protocol Router Network (SIPRNet) that contains individual PKI certificates used for network logon, Web site authentication, and secure e-mail.

Tempest – an unclassified term referring to technical investigations for compromising emanations from electrically

operated information processing equipment; these investigations are conducted in support of emanations and emissions security.

APPENDIX C – ACRONYMS

ACS	Access Control System
ANSI	American National Standards Institute
AO	Authorizing Officials
AT/FP	Antiterrorism/Force Protection
BOD	Board of Directors
BRAC	Base Realignment and Closure Act
CAA	Controlled Access Area
CAC	Common Access Card
CCRI	Command Cyber Readiness Inspection
CDN	Computer Network Defense
CDO	Command Duty Officer
CIO	Chief Information Officer
CJCSI	Chairman Joint Chiefs of Staff Instruction
CLAN	Classified Local Area Network
CMWD	Commercial Mobile and Wireless Device
CNIC	Commander, Navy Installations Command
CNO	Chief of Naval Operation
CO	Commanding Officer
COMCEN	Communication Center
CSA	Cognizant Security Authority
CSM	Command Security Manager
CTTA	Certified TEMPEST Technical Authority
CY	Calendar Year
DAA	Designated Approving Authority DHS Department of Homeland Security
DIRSSP	Director, Strategic Systems Programs
DISN	Defense Information Systems Network
DO	Duty Officer
DoD	Department of Defense
DON	Department of the Navy
DRRS-N	Defense Readiness Reporting System-Navy
DSS	Defense Security Service
DTM	Directive Type Memorandum
ERP	Enterprise Resource Planning
FDC	Facility Design Criteria
GIG	Global Information Grid

GSA	General Services Administration
HQ	Headquarters
IA	Information Assurance
IA PUB	Information Assurance Publication
IAM	Information Assurance Manager
ID	Identification
IDE	Intrusion Detection Equipment
IDS	Intrusion Detection System
IG	Inspector General
IR	Infrared
ISP	Information Security Program
IT	Information Technology
ITAO	Interim Authorization to Operate
JAGMAN	Judge Advocate General Manual
LAA	Limited Access Area
MILCON	Military Construction
MIS	Management Information System
NAC	Nebraska Avenue Complex
NAVFAC	Naval Facilities Engineering Command
NAVINSGEN	Office of the Naval Inspector General
NCIC	National Crime Information Center
NHHC	Naval History and Heritage Command
NIGHTS	Naval Inspector General Hotlines Tracking System
NIPO	Navy International Programs Office
NIPR	Non-secure Internet Protocol Router Network
NSA	National Security Agency
NSAW	Naval Support Activity, Washington
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OGC	Office of the General Counsel
OIC	Officer in Charge
OJAG	Office of the Judge Advocate General
OSC	Office of Special Counsel
OSS	Open Storage Secret Area
PCS	Personal Communications System
PDC	Protected Distribution Center
PDS	Protective Distribution System
PED	Personal Electronic Device
PIV	Personal Identity Verification

POAM	Plan of Action and Milestone
PSRB	Physical Security Review Board
RAA	Restricted Access Area
RF	Radio Frequency
RFP	Request for Proposal
SECDEF	Secretary of Defense
SECNAV	Secretary of the Navy
SECVIO	Security Violation
SF	Standard Form
SIPR	Secret Internet Protocol Router
SIPRNET	Secret Internet Protocol Router Network
SP10	Strategic Systems Programs Director, Plans and Programs
SP16	Strategic Systems Programs Management Information and Support Services Branch Head
SP50	Strategic Programs Royal Navy Branch
SPAWARSYSCEN	Space and Naval Warfare Systems Command
SSP HQ	Strategic Systems Programs Headquarters
SR	Secure Room
SR	Secure Room
SSP	Strategic Systems Program
SSPINST	Strategic Systems Programs Instruction
STC	Sound Transmission Class
STIG	Security Technical Implementation Guide
TEMPEST	Transient Electromagnetic Pulse Surveillance Technology
UAA	Uncontrolled Access Area
UK	United Kingdom
USCC	United States Cyber Command
USMC	United States Marine Corps
WNY	Washington Navy Yard

APPENDIX D – INTERVIEWS CONDUCTED

W 41 – Facility Manager, Public Works (Witness)
W 5 - Director, SSP; Washington, DC (Witness)
W 20 - Deputy Director, SSP; Washington, DC (Witness)
W 40 - Special Agent, Naval Criminal Investigative Service, Camp Lejeune, NC
W 42 - Requirements Branch Head, Naval Facility Engineering Command Washington (Witness)
W 35 - Project Manager, Naval Facility Engineering Command Washington (Witness)
W 25 - Deputy, Command Information Officer, SSP; Washington, DC (Witness)
EDWARDS, Sparky – Former Security Manager, SSP; Washington, DC (Whistleblower)
W 43 - Nuclear Weapons Security Officer, SSP; Washington, DC (Witness)
W 19 - Deputy Director, Plans and Programs, SSP; Washington, DC (Witness)
W 28 - Security Specialist, SSP; Washington, DC; (Witness)
W 33 - Chief of Security, Department of Defense - Defense Security Service, Quantico, VA (Witness)
W 17 - Command Information Officer, SSP; Washington, DC (Witness)
W 10 - Head, Management and Information Services Officer, SSP; Washington, DC (Witness)
W 9 - Division Director, Plans and Programs, SSP; Washington, DC (Witness)
W 44 - Project Manager, Naval Facilities Engineering Command, Washington, DC (Witness)
LONDAGIN, Vernon – Former Deputy Security Manager, SSP; Washington, DC (Whistleblower)
W 18 - Contractor, Architect and Facilities Manager, SSP; Washington, DC (Witness)
W 30 - Security Specialist, SSP; Washington, DC (Witness)
W 16 - Special Security Manager, SCI, SSP; Washington, DC (Witness)
W 45 - Contractor, Facilities Specialist, SSP; Washington, DC (Witness)
W 32 - Security Specialist, Defense Security Services, Quantico, VA (Witness)

W 1 – Facility Acquisition and Environmental, SSP Project Manager/Lead, SSP; Washington, DC (Witness)
W 46 – Industrial Security Specialist, SSP; Washington, DC (Witness)
W 38 - Commanding Officer, Naval Support Activity Washington; Washington, DC (Witness)
IO 2 – Intelligence Officer, Office of the Naval Inspector General, Washington DC (Witness)

**Employee Retired in December 2011 - Letter Requesting to Interview mailed to Home of Record on May 6, 2014*

APPENDIX E - DOCUMENTS EXAMINED

Allegation One

18 U.S. Code 1382, Section 930

50 U. S. Code 797

CNIC Instruction 5530.14A CNIC Ashore Protection Program, 29 May 2013

CNO Washington DC NAVADMIN 146/13 29 May 2013

DoD 5200.08R PHYSICAL SECURITY PROGRAM, April 9, 2007, Incorporating Change 1, May 27, 2009

DoD Instruction 5200.08 Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB) December 10, 2005, Incorporating Change 2, Effective April 8, 2014

JAGMAN INVESTIGATION INTO THE FATAL SHOOTING INCIDENT AT THE WASHINGTON NAVY YARD (WNY) ON 16 SEPTEMBER 2013 AND ASSOCIATED SECURITY, PERSONNEL, AND CONTRACTING POLICIES AND PRACTICES, 5800 N00ND of 8 Nov 2013

MEMORANDUM FOR THE SECRETARY OF DEFENSE, Subject: Investigation of the Fatal Shooting Incident at the Washington Navy Yard on September 16, 2013, 12 November 2013

NSAWINST 5532.1 Procedures for Vetting Visitors to Navy Museum

OPNAVINST 3501.360 Protected Operational Environment and required Operational Capabilities, 28 January 2008

OPNAVINST 5530.14E CH-1, NAVY PHYSICAL SECURITY AND LAW ENFORCEMENT PROGRAM, 19 Apr 2010

Public Law 110-181 Section 1069
SECNAVINST M-5510, Department of the Navy Information Security Program, June 2006

Statement by the Honorable Ray Mabus, Secretary of the Navy, Washington Navy Yard JAGMAN Press Conference, Washington DC, 18 March 2014

UNDER SECRETARY OF DEFENSE MEMORANDUM Directive-Type Memorandum (DTM) 09-012, "Interim Policy Guidance for DoD Physical Access Control" December 8, 2009 Incorporating Change 4, April 22, 2014

History and Heritage Command Website, http://www.defense.gov/pubs/DoD-Internal-Review-of-the-WNY-Shooting-20-Nov-2013.pdf

Allegation Two

In addition to those cited by Allegation Two:

Appointment letter for Strategic Systems Programs Command Security Manager, From: Director, Strategic Systems Programs, To: Mr. Sparky Edwards, 29 Jun 2012

Attachment to E-mail 1 Mar 2013 From: Mr. Edwards, To: W9 From Command Security Manger, Strategic Systems Programs, Subject: Security-In-Depth Determination, 1 Mar 2013

W6 Checklist, Facility/Building Storage Checklist for W200 Rooms 4103 and 4103,4 August 2011

CHECKLIST, CONTROLLED ACCESS AREA (CAA), Standard Form

CHECKLIST, CONTROLLED ACCESS AREA (CAA), Strategic Systems Programs, Room 3100, 01 Feb 2013

CHECKLIST, CONTROLLED ACCESS AREA (CAA), Strategic Systems Programs, Doors on 3rd Floor, 01 Feb 2013

CHECKLIST, CONTROLLED ACCESS ARES (CAA), Strategic Systems Programs, ALL, 1 Mar 2013

CHECKLIST, CONTROLLED ACCESS AREA (CAA), Strategic Systems Programs, attached to Mr. Edwards' e-mail to W9 , dated 1 Mar 2013

CHECKLIST, RESTRICTED ACCESS AREA (RAA), Standard Form

CHECKLIST, SECURE ROOM (SR) CHECKLIST, OPEN STORAGE SECRET (COLLATERAL), Standard Form

DEPARTMENT OF THE NAVY, OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION INTERVIEW OF W14 , 16 Jul 2014

DEPARTMENT OF THE NAVY, OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION INTERVIEW OF Messrs. Sparky Edwards and Vernon Londagin, 18 Dec 2013

DEPARTMENT OF THE NAVY, OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION INTERVIEW OF W 17 , Date Unknown

DEPARTMENT OF THE NAVY, OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION INTERVIEW OF W 18 , 201

W 10 Interview Testimony Regarding SIPR and Personnel Electronic Devices Date Unknown

E-mail: From: W 47 , To: IO 3 , Subject: FW: SSP's CAA, 24 Jul 2014

E-mail: From: W 47 , To: IO 3 , Subject: FW: Problem that I need help with ASAP Please…SSP CAA POA 25 Jul 2014, original 6 Feb 2013

E-mail: From: Edwards, Sparky, To: W 10 , Subject: The CAA Standing for the SSP, 6 Jun 2012

E-mail: From: W 9 To: W 24 , Subject: Security Issues SP162, 5 Nov 2013

E-mail: From: IO 2 , To: IO 4 , IO 3 , IO 5 , Subject: FW: SIPR (Protected Communication), 23 Jul 2014, copy of Mr. Edwards 18 Mar 2013 e-mail to W 10 regarding SIPR violations

E-mail: IO 2 , N2B
To: IO 3 ; IO 6 CIV N3B; IO 5
Subject: FW: Command Security Discussion -- 24 JAN 2013, 23 Jul 2014

Excel Spreadsheet of Security Issues, Provided by Mr. Edwards to W 9 , 5 Mar 2013

INTERIM POLICY CHANGES, REMINDERS AND CLARIFYING GUIDANCE TO SECNAV M-5510 .36, 5510, Ser N09N2/9U223112, MAY 012009

INTERIM POLICY CHANGE TO REQUIREMENTS FOR A SECURE ROOM USED FOR OPEN STORAGE SECRET AND DESIGNATION OF SECURE ROOMS, CONTROLLED ACCESS AREA AND RESTRICTED ACCESS AREA, 5510, Ser N09N2/10U213104, 16 Mar 2010

MEMORANDUM, Subject: Strategic Systems Programs Headquarters (SPHQ) Controlled Access Areas (CAA)/Restricted Access Area (RAA) Certification, 11 Mar 2011

MEMORANDUM, Subject: Designation of Secure Room For Open Storage of Secret Material, 5510 SP16/SerU03213001, 20 Mar 2013

MEMORANDUM FOR THE RECORD, SP205 Secure Room Certification, 21 Dec 2010

MEMORANDUM FOR THE RECORD SP202 Secure Room (SR) Certification, 3 March 2011

Naval Inspector General, Command Inspection of Strategic Systems Programs, 23-31 January 2013

Physical Security Assessment and Certification for Strategic Systems Programs Building 200, 5510, Ser 08061100000, 5 Aug 2011

Third Floor Security Floor Plan (architectural)

Position Description, Supervisory Systems Programs, 17 Oct 2011

SECNAV M-5510.36 Department of the Navy Information Security Program, June 2006

Strategic Systems Program Office, Case #OSC 2348 & 2349, NIGHTS 201303073, Interview Questions, Interviewee: W 10 , GS15, Branch Head SP16, 13 Jan 2014

Strategic Systems Program Office, Case #OSC 2348 & 2349, NIGHTS 201303073, Interview Questions, Interviewee: W 16
Special Security Representative (SSO), 13 Jan 2014

SSP CAA POA, From: SP162, To: Sp1624, Subject: SSP Controlled Access Area Plan of Action, 6 Feb 2013

SSP Work Requests, 5 Jan 11

SSP INSTRUCTION 5510.16D, Strategic Systems Programs Security Manual, 3 Jan 2014

SSP Official Newsletter, SPHQ SIPRNET Operations, February 2013

UNITED STATES NAVY/UNITED STATES MARINE CORPS (USN/USMC)

INFORMATION ASSURANCE (IA) PUBLICATION MODULE 5239-22 INFORMATION ASSURANCE, PROTECTED DISTRIBUTION SYSTEM (PDS) PUBLICATION, September 2008

Allegation Three

In addition to those cited by Allegation Two,

Chairman of the Joint Chiefs of Staff Instruction, Information Assurance,(CJCSI) 6510.01F 9 Feb 2011

CJCSI 6211.02d, Defense Information Systems Network Responsibilities, 24 January 2012

Security Technical Implementation Guide CS-040 Protected Distribution System Construction

Allegation Four

DEPARTMENT OF THE NAVEY OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION, INTERVIEW OF W 5 , 19 February 2014

DEPARTMENT OF THE NAVEY OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION, INTERVIEW OF W 19 , 16 July 2014

DEPARTMENT OF THE NAVEY OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION, INTERVIEW OF W 33 , 19 May 2014

DEPARTMENT OF THE NAVEY OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION, INTERVIEW OF W 17 , DATE UNKNOWN

DEPARTMENT OF THE NAVEY OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION, INTERVIEW OF W 10 , DATE UNKNOWN

DEPARTMENT OF THE NAVEY OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION, INTERVIEW OF W 32 , DATE UNKNOWN

E-mail: From: W 25 , To: IO 7 , Subject: FW: Security Inspection, 28 April 2014

E-mail: From: W 32 , To: Edwards, Sparky, W 48 , W 49 , W 40 , Subject: RE;I am in a JAm, 14 March 2013

E-mail: From: W 21 , From: Edwards, Sparky, Subject: RE: FOR REVIEW: DIRSSP Bi-Weekly, 12 March 2013

E-mail: From: W 24 , To: IO 1 , Subject: FW:URGENT REQUEST – Cyber Inspection Timeline, 28 July 2014

Ser 10/U012312000, Subject: Request for Cyber Security Inspection Schedule Change

Allegation Five

DoDD, 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 14 April 2004, Certified Current as of April 23, 2007

DEPARTMENT OF THE NAVY, OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION INTERVIEW OF W 40 , 12 May 2014

DEPARTMENT OF THE NAVY, OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION INTERVIEW OF W 14 , 16 Jul 2014

DEPARTMENT OF THE NAVY, OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION INTERVIEW OF Messrs. Sparky Edwards and Vernon Londagin, 18 Dec 2013

DEPARTMENT OF THE NAVY, OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION INTERVIEW OF W 17 , Date Unknown

DEPARTMENT OF THE NAVY, OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION INTERVIEW OF W 28 , Date Unknown

DEPARTMENT OF THE NAVY, OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION INTERVIEW OF W 18 , 2014

DEPARTMENT OF THE NAVY, OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION INTERVIEW OF W 1 , 16 July 2014

E-mail: From: W 24 , To: IO 8 , Subject: RE: BOD CHARTER INSTRUCTION, 24 July 2014

MEMORANDUM FOR THE RECORD SP202 Secure Room (SR) Certification, 3 March 2011

MEMORANDUM, Subject: Strategic Systems Programs Headquarters (SPHQ) Controlled Access Areas (CAA)/Restricted Access Area (RAA) Certification, 11 Mar 2011

Office of Special Counsel, To: The Honorable Chuck Hagel, Secretary, Department of Defense, RE: OCS File Nos. DI-20301-1400, 25 September 2013

Physical Security Assessment and Certification for Strategic Systems Programs Building 200, 5510, Ser 08061100000, 5 Aug 2011

SECNAVINST M-5510, Department of the Navy Information Security Program, June 2006

SECVIO 03012013-008, From; Sp162, To: SP01, Subject: Security Violation

SSP Instruction 5230.14, Subject: Commercial Mobile and Wireless Device, Service and Technology Policy, 19 Nov 2013

SSP Instruction 8100.1, Subject: Cellular/Personal Communication System (PCS) Devices Policy at Strategic Systems Programs Headquarters, 30 May 2008

Strategic Systems Program Office, Case #OSC 2348 & 2349, NIGHTS 201303073, Interview Questions, Interviewee: W 16 , GS15, Branch Head SP16, 13 Jan 2014

Allegation Six

Appointment letter for Strategic Systems Programs Command Security Manager, From: Director, Strategic Systems Programs, To: Mr. Sparky Edwards, 29 Jun 2012

W 14

Department of the Navy, Voluntary Statement, 28 Jul 2014

W 51 W 19

E-mail: From: , To: , Subject: Proposed Plan for Daily Security Checks Within 5200 Spaces, 9 Oct 2012

SECNAVINST M-5210.0, Department of the Navy Records Management Manual, Nov 2007

SECNAVINST M-5510, Department of the Navy Information Security Program, June 2006

W 50

Summarized Interview Results ICO , USN, RE: OSC Tasker 23092348, 25 July 2014

IO 9

Statement, , USN, RE: OSC Tasker 23092348, 29 July 2014

Statement, W 10 to IO 9 , IO 10 and W 16
25 Jul 2014

Strategic Systems Program Office, Case #OSC 2348 & 2349, NIGHTS 201303073, Interview Questions, Interviewee: W 19 , GS-15, Deputy Director, Plans and Programs, 22 Nov 2013

SSP Instruction, Subject: Common Access Card Policy, 19 Feb 2013

SSP Instruction 5230.14 for Commercial Mobile and Wireless Services 19 November 20313

Allegation Seven

Correspondence: From: W 29 , To: Sparky Edwards, Re: W 51
15 Mar 2013

GENADMIN, DON CIO, Subject: Acceptable Use Policy for Department of the Navy (DON0 Information Technology (IT) Resources, 3 Oct 2011

UNITED STATES NAVY/UNITED STATES MARINE CORPS (USN/USMC) INFORMATION ASSURANCE (IA) PUBLICATION MODULE 5239-22 INFORMATION ASSURANCE, PROTECTED DISTRIBUTION SYSTEM (PDS) PUBLICATION, September 2008

Allegation Eight

Appointment letter for Strategic Systems Programs Command Security Manager, From: Director, Strategic Systems Programs, To: Mr. Sparky Edwards, 29 Jun 2012

Correspondence: From: SP160, To: SP10, Subject SP50 Washington Navy Yard Physical Security Concerns, 25 April 2011

E-mail: From W 6 , To: W 35 , Subject: LENEL SYSTEMS FAILURES, 13 Jan 2011

E-mail: From: W 14 , To: IO 11 , Subject: Re: Questions about Security Manager Qualifications and Certifications, 25 Jul 2014

E-mail: From: Edwards, Sparky, To: W 12 , Subject: Afterhours Inspection 08052012, 5 Sept 2012

E-mail: From: W 10 , To: W 24 , Subject: FW: Info on Building 200 guards, 22 Jul 2014

E-mail: From: W9 , To: W11 , Subject: Building Security, 1 Sept 2011

E-mail: From: W9 , To: W24 , Subject: FW SECDIS 10202012-3, 5 Nov 2013

E-mail: From: W9 , To: W24 , Subject: FW: Security Issues List, 5 Nov 2013

E-mail: From: W9 , To: W24 , Subject: FW follow up, 5 Nov 2013

Excel Spreadsheet of Security Issues, Provided by Mr. Edwards to W9 , 5 March 2013, with Status Update Attached, 22 July 2014

MEMORANDUM FOR THE RECORD SP202 Secure Room (SR) Certification, 3 March 2011

Naval Inspector General, Command Inspection of Strategic Systems Programs, 23-31 January 2013

Position Description, Supervisory Systems Programs, 17 Oct 2011

Resignation Letter, From: Sparky D. Edwards, To: Director, Strategic Systems Programs, 21 Mar 2013

Strategic Programs Royal Navy MEMORANDUM, From: Sp50/Sp5041, To: SP10 – W9 , Subject: Washington Navy Yard Physical Security Concerns, 23 Mar 2011

SSP Board of Directors (BOD) Roles and Responsibilities: Oversight of SSP's Program/Budget Reviews- A Key Program Management Discipline, July 2011

Strategic Systems Program Office, Case #OSC 2348 & 2349, NIGHTS 201303073, Interview Questions, Interviewee: W5 , W5 , Strategic System Program, 19 Feb 2014

Strategic Systems Program Office, Case #OSC 2348 & 2349, NIGHTS 201303073, Interview Questions, Interviewee: W9 , Director, Plans and Programs, Senior Executive Service Member, 16 Jan 2014

Strategic Systems Programs Official Newsletter, 25 Feb 2013

Miscellaneous

Assessment Control #13-DCWA-0343-5XNA/C (September 2013)

Authorization to Operate the SSP Classified Local Area Network TO Accreditation June 2012

Authorization to Operate the SSP Classified Local Area Network TO Accreditation September 2011

Controlled Access and Restricted Access Areas Certification

E-mail Regarding Waivers March 2013 for Mr. Sparky Edwards

Information Assurance Publication, 5239-22, September 2008

Interim Authorization to Operate the SSP Classified Local Area Network TO Accreditation May 2011

Interim Authorization to Operate the SSP Classified Local Area Network TO Accreditation December 2010

Naval Criminal Investigative Service (NCSI) Investigation

NAVINSGEN Senior Official Case #12-127399 (September 2013)

Prohibition from Entry On Naval Support Activity Washington DC

Prohibition from Entry On Naval Support Activity Washington DC for Mr. Vernon Londagin

Public Law 108-268 - Transfer of Nebraska Avenue Naval Complex, District of Columbia

SSP Secure Room Certifications

SSP Security Technical Implementation Guide (STIG) (Basic, NIPR, and SIPR)

Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)

SSP Building Work List Requirements January 2011

SSP Door Modification for CAA Certification WO#1322414

SSP Facility Design Criteria MILCON Project P402C

SSP Hotline Investigation 201300707 (March 2013)

SSP Hotline Investigation 201300727 (September 2013)

SSP Management Inquiry (September 2013)

SSP Move Memorandum - Deputy Assistant Secretary of the Navy

SSP Open Storage Secret Material Designation

SSP Security Manual January 2014

Summary of Testimony

DEPARTMENT OF THE NAVEY OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION, INTERVIEW OF W 5 19 February 2014

DEPARTMENT OF THE NAVY, OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION INTERVIEW OF W 40 , 12 May 2014

DEPARTMENT OF THE NAVY, OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION INTERVIEW OF W 14 , 16 Jul 2014

DEPARTMENT OF THE NAVY, OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION INTERVIEW OF Messrs. Sparky Edwards and Vernon Londagin, 18 Dec 2103

DEPARTMENT OF THE NAVEY OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION, INTERVIEW OF W 19 , 16 July 2014

DEPARTMENT OF THE NAVY, OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION INTERVIEW OF W 28 , Date Unknown

DEPARTMENT OF THE NAVEY OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION, INTERVIEW OF W 33 , 19 May 2014

DEPARTMENT OF THE NAVY, OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION INTERVIEW OF W 17 , Date Unknown

DEPARTMENT OF THE NAVY, OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION INTERVIEW OF W 18 , 2014

DEPARTMENT OF THE NAVEY OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION, INTERVIEW OF W 32 , DATE UNKNOWN

DEPARTMENT OF THE NAVY, OFFICE OF THE INSPECTOR GENERAL, DIGITAL TRANSCRIPTION INTERVIEW OF W 1 , 16 July 2014

W 17 Interview Testimony Regarding SIPR and Personnel Electronic Devices Date Unknown

Summarized Interview Results ICO W 50 , USN, RE: OSC Tasker 23092348, 25 July 2014

Strategic Systems Program Office, Case #OSC 2348 & 2349, NIGHTS 201303073, Interview Questions, Interviewee: W 5
Vice Admiral/Director, Strategic System Program, 19 Feb 2014

Strategic Systems Program Office, Case #OSC 2348 & 2349, NIGHTS 201303073, Interview Questions, Interviewee: W 10 , GS15, Branch Head SP16, 13 Jan 2014

Strategic Systems Program Office, Case #OSC 2348 & 2349, NIGHTS 201303073, Interview Questions, Interviewee: W 9 , Director, Plans and Programs, Senior Executive Service Member, 16 Jan 2014

Strategic Systems Program Office, Case #OSC 2348 & 2349, NIGHTS 201303073, Interview Questions, Interviewee: W 16
Special Security Representative (SSO), 13 Jan 2014