



DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

OFFICE OF THE ASSISTANT SECRETARY

SAF/MR
1660 Air Force Pentagon
Room 4E1010
Washington, DC 20330-1660

The Honorable Henry J. Kerner
Special Counsel
United States Office of Special Counsel
1730 M Street N.W., Suite 300
Washington, DC 20036-4505

Re: OSC File No. DI- 21-000551

Dear Mr. Kerner:

As agency head, the Secretary of the Air Force delegated to me his authority to review, sign, and submit to you the report required by Title 5, U.S.C. Section 1213(c) and (d). I am responding to your June 25, 2021 correspondence, referring for investigation whistleblower disclosures from [REDACTED] alleging that employees at Air National Guard, Eastern Air Defense Sector (EADS), 224th Support Squadron, Rome, New York, "engaged in actions that constitute a violation of law, rule, or regulation; gross mismanagement; and a substantial and specific danger to public safety." After a clarification with the complainant, the Department investigated six allegations against one subject, the Officer in Charge, of the 224th Support Squadron. The six allegations were:

Allegation 1: Between 27 January 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, failed to implement countermeasures to the Patriot Excalibur (PEX) servers, to mitigate "critical or high risk" vulnerabilities identified as Tier I in violation of AFI 17-130, *Cybersecurity Program Management*.

UNSUBSTANTIATED

Allegation 2: Between 1 February 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, failed to implement a backup system of Classified and Unclassified (RADIUS) systems increasing the probability of "catastrophic" data loss impacting National Security Systems in violation of AFI 17-130, *Cybersecurity Program Management*. **UNSUBSTANTIATED**

Allegation 3: Between 27 January 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, failed to track secured hard drives containing classified information in violation of AFI 17-1203, *Information Technology Asset Management*. **UNSUBSTANTIATED**

Allegation 4: Between on or about 1 February 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, directed the improper disposal of classified IT hardware, in violation of AFMAN 17-1301, *Computer Security (COMPUSEC)*. **UNSUBSTANTIATED**

Allegation 5: Between on or about 27 January 2021 and 5 Feb 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, directed the destruction of government property, to wit: usable, unclassified desktops and laptops still under warranty, in violation of AFI 17-1203, *Information Technology Asset Management*. **UNSUBSTANTIATED**

Allegation 6: Between 27 January 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, failed to provide communication and information system records (CISR) documentation to Technicians for National Security Systems in violation of AFI 17-101 para. 3.12.3, *Risk Management Framework for Air Force Information Technology*. **UNSUBSTANTIATED**

The appointed Investigating Officer (IO) completed an extensive investigation, during which she interviewed the complainant, the identified subject, six witnesses, and obtained documentary evidence.

The preponderance of the evidence supports the IO's determination that Allegation 1 is unsubstantiated. The IO was reasonable in determining, based on the preponderance of evidence, that no violation of rule, law, or regulation had occurred. Witness testimony and documentary evidence support the IO's finding that there was continuous monitoring of security control implementation on the PEX server, that the Cyber Security program involved several echelons of engagement, specifically designed to mitigate "high risk" vulnerabilities, and that the subject, in accordance with (IAW) AFI 17-101, *Risk Management Framework (RMF) For Air Force Information Technology (IT)*, conducted a functional mission analysis given the role of the system in the unit, security protocols, impact, staff, and the unit's priority of effort at the time.

As for Allegation 2, the IO was reasonable in determining, based on the preponderance of evidence that no violation of rule, law, or regulation had occurred. The evidence indicates the RADIUS servers provided defense to the network with the additional authentication capability, but did not actually store any data; therefore, there could be no catastrophic data loss.

The IO was also reasonable in not substantiating Allegation 3 that the subject failed to track secured hard drives containing classified information in violation of AFI 17-1203,

Information Technology Asset Management. The evidence showed that the Equipment Control Officer (ECO) was responsible for the disposal of classified items, which were tracked in a database of asset inventory called DPAS and that the subject was not the ECO.

The preponderance of the evidence also supports the IO's determination that Allegation 4 that the subject directed the improper disposal of classified IT hardware, in violation of AFMAN 17-1301, *Computer Security (COMPUSEC)* is not substantiated. The IO was reasonable in determining, based on the preponderance of evidence that no violation of rule, law, or regulation had occurred. Evidence showed that a moratorium of assets prevented the turn-in and physical inventory of equipment from 9 May 2020 until after 31 March 2021. The DRMO responsible management official is the ECO and the subject was not the ECO. Additionally, although the subject had oversight authority over Cyber Systems Support (SCOO), the subject was not responsible for the disposal of classified IT equipment and did not have the authority to direct the DRMO prescribed disposal process IAW AFI 17-1203.


Regarding Allegation 5, that the subject directed the destruction of government property, to wit: usable, unclassified desktops and laptops still under warranty, the IO was reasonable in determining this allegation was not substantiated. The ECO recalled an incident involving a laptop under warranty that was mistakenly collected for turn-in. However, the ECO testified that it was his responsibility to look at the warranty expiration date. There were no witnesses who could attest to having heard the subject direct the improper disposal of IT under warranty.

Finally, the preponderance of the evidence supports the IO's determination that Allegation 6 that the subject failed to provide communication and information system records (CISR) documentation to Technicians for National Security Systems in violation of AFI 17-101 para. 3.12.3, *Risk Management Framework for Air Force Information Technology*, is not substantiated. There was no evidence to indicate that the subject was responsible for ensuring the CISR document was updated. Evidence indicated that in the 224th Support Squadron, the SCXP IT Specialist is responsible. While evidence was presented that the SCOO Work Center failed to provide the minimally required updates, the subject was not aware of the inaccuracy of this specific work center's CISR drawings. The IO was reasonable in determining that no violation of rule, law, or regulation had occurred.

I am enclosing the Report of Investigation for your official use. I understand you will provide the full copy of this Report and Addendum to the President and the House and Senate Armed Services Committees for their review and to [REDACTED]. As directed by the Office of Special Counsel in its Appendix to the June 25, 2021 referral letter, we will also provide a redacted version of the Report in which agency employees are identified by position title vice name with an attached key identifying the employees by name and position. The redacted copies will be published on your webpage.

We appreciate your efforts to bring this matter to our attention. If the Department of the Air Force can be of any further assistance, please contact [REDACTED] Associate

General Counsel, Fiscal, Ethics and Administrative Law at [REDACTED] or
[REDACTED]

A handwritten signature in black ink, consisting of a large, stylized loop followed by a horizontal stroke that tapers to the right.

ALEX WAGNER
Assistant Secretary
(Manpower and Reserve Affairs)

CUI

REPORT OF INVESTIGATION

PREPARED BY



224th Support Squadron, Eastern Air Defense Sector (EADS)

**CONCERNING ALLEGATIONS OF “MISMANAGEMENT and IMPROPER
AUTHORIZATION”**

24 JUNE 2022

Controlled by: Department of the Air Force
Controlled by: DAF/IG
CUI Category: CUI//PRIIG
Distribution/Dissemination Control: FEDCON
POC: michael.donahue@us.af.mil

Section II, Tab A. -- Executive Summary.

Introductory Paragraph. In a letter dated June 25, 2021 and signed by the Special Counsel, the Office of Special Counsel (OSC) referred to the Secretary of the Air Force (SECAF) for investigation whistleblower disclosures alleging that employees at Air National Guard, Eastern Air Defense Sector (EADS), 224th Support Squadron, Rome, New York, “engaged in actions that constitute a violation of law, rule, or regulation; gross mismanagement; and a substantial and specific danger to public safety.” According to OSC, the whistleblower, [REDACTED] (Complainant) is the former IT Lead (GS-12) of Air National Guard, Eastern Air Defense Sector (EADS), 224th Support Squadron, Rome, New York. Complainant has consented to the release of his name, and disclosed several allegations that “reported serious information security failures and mismanagement within the EADS” at a mission-critical facility in Rome, New York. We initiated this investigation in response to allegations that:

Allegation 1: Between 27 January 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, failed to implement countermeasures to the Patriot Excalibur (PEX) servers, to mitigate “critical or high risk” vulnerabilities identified as Tier I in violation of AFI 17-130, *Cybersecurity Program Management*.

Findings. The Patriot Excalibur (PEX) server is being used primarily to support scheduling and planning missions for operators. While it is not deemed critical for weapons systems, it is critical to associated support functions. While Subject has an oversight role over the PEX server, he was not responsible for day-to-day operations involving PEX. Witness testimonies indicate that there are layers of security controls to protect PEX servers from vulnerabilities. The IO found no evidence that the Subject failed to address critical vulnerabilities in violation of a rule, law or regulation.

Substantiation. NOT SUBSTANTIATED.

Allegation 2: Between 1 February 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, failed to implement a backup system of Classified and Unclassified (RADIUS) systems increasing the probability of “catastrophic” data loss impacting National Security Systems in violation of AFI 17-130, *Cybersecurity Program Management*.

Findings. The RADIUS servers were a layer of defense to the business systems on the networks, not its mission systems. The Subject was not in a technical role to advise on the implementation of a backup system as a Supervisor, however, as the Flight Commander, the Subject could set the priorities. The RADIUS servers provided defense to the network with the additional authentication capability and did not actually lose any data, therefore, could not result in

catastrophic data loss. There was no evidence that the Subject violated a rule, law, regulation or standard.

Substantiation. NOT SUBSTANTIATED.

Allegation 3: Between 27 January 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, failed to track secured hard drives containing classified information in violation of AFI 17-1203, *Information Technology Asset Management*.

Findings. The Equipment Control Officer (ECO) and other witnesses detailed the process prescribed in AFI 17-203 for the handling of classified materials. Each witness indicated that the unit took the handling of classified materials seriously and indicated that, if alerted, would seek assistance from a higher authority, as mishandling of classified materials is a security incident. No evidence was presented to support the allegation that the Subject directed the improper disposal of hard drives, therefore, the IO found that no policy, rule, law, or regulation was violated.

Substantiation. NOT SUBSTANTIATED.

Allegation 4: Between on or about 1 February 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, directed the improper disposal of classified IT hardware, in violation of AFMAN 17-1301, *Computer Security (COMPUSEC)*.

Findings. The Complainant provided anecdotal evidence that was not supported by witness statements or surrounding facts. There was no evidence of loss as a result of the modified procedures. The directives that govern the proper disposal of serialized classified IT equipment prescribe a process that requires the cooperation of the hand-receipt holder, the individual disposing of the equipment, and the (ECO). There is no substantive link to the Subject and the improper disposal of classified IT equipment. Based on the preponderance of evidence, the Subject violated no rule, law, or regulation.

Substantiation. NOT SUBSTANTIATED.

Allegation 5: Between on or about 27 January 2021 and 5 Feb 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, directed the destruction of government property, to wit: usable, unclassified desktops and laptops still under warranty, in violation of AFI 17-1203, *Information Technology Asset Management*.

Findings. There is insufficient evidence to support the allegation that the Subject directed the destruction of IT assets (i.e. desktops and laptops) under warranty. The Subject denied directing the destruction of any IT equipment, and no direct evidence was found to support that he may have directed such an action. Based on a preponderance of evidence, the IO determined that no violation of rule, law, or regulation occurred.

Substantiation. NOT SUBSTANTIATED.

Allegation 6: Between 27 January 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, failed to provide communication and information system records (CISR) documentation to Technicians for National Security Systems in violation of AFI 17-101 para. 3.12.3, *Risk Management Framework for Air Force Information Technology*.

Findings. The CISR document, a compilation of work center drawings depicting the base communications infrastructure, is updated annually by designated points of contacts within each work center. The Subject was not responsible for ensuring that the CISR document was updated. That role was assigned to an IT Specialist within the Plans and Programs work center, although in accordance with the standard, the role is reserved for the Information Security System Manager (ISSM). Evidence was presented that the designated point of contact for the Cyber Systems Support failed to provide the minimally required updates, however, the Subject was not made aware of the issue. Based on the preponderance of evidence, the Subject did not violate a rule, law, or regulation.

Substantiation. NOT SUBSTANTIATED.

Recommendation. We make no recommendations in these matters.

Section II, Tab B -- Background, Scope and Statutory Authority.

The Air National Guard provides the majority of the forces for the North America Aerospace Defense Command (NORAD) mission. Specifically, the New York Air National Guard's 224th Air Defense Group (224 ADG) provides a significant amount of personnel in support of the mission. The 224 ADG consists of the 224th Air Defense Squadron (224 ADS), the 224th Support Squadron (224 SS) and two detachments in the Washington, D.C. area. The 224 SS, an O-6 level command, has a Director of Operations, two Assistant Director of Operations, and seven subsections to include: Security Forces (SFF), Logistics and Engineering (LGR), Plans and Resources (SCX), Cyber Mission Systems (SCP), Cyberspace Operations (SCO), Cyberspace Quality Assurance (QA), and Drill Status Guard (DSG) Cyber Officers. [REDACTED], the Complainant, was a member of the Cyber Systems Support (SCOO), a subsection of Cyberspace Operations (SCO). SCOO consisted of the Network Operations (NetOps) and the Client Service Center.

In a letter dated June 25, 2021 and signed by the Special Counsel, the Office of Special Counsel (OSC) referred to the Secretary of the Air Force (SECAF) for investigation whistleblower disclosures alleging that employees at Air National Guard, Eastern Air Defense Sector (EADS), 224 SS, Rome, New York, "engaged in actions that constitute a violation of law, rule, or regulation; gross mismanagement; and a substantial and specific danger to public safety." According to OSC, the whistleblower, [REDACTED] (Complainant) is the former IT Lead (GS-12) of Air National Guard, EADS, 224 SS, Rome, New York. Complainant has consented to the release of his name, disclosed several allegations and "reported serious information security failures and mismanagement within the EADS" at a mission-critical facility in Rome, New York. After review and based on the information disclosed by the whistleblower, OSC "concluded that there is a substantial likelihood that the information provided to OSC discloses a violation of law, rule or regulation; gross mismanagement; and a substantial and specific danger to public safety."

According to the OSC Referral Letter, the allegations to be investigated include:

Officer in Charge, [Subject], and other EADS officials, have intentionally ignored numerous vulnerabilities within mission-critical systems, leaving the squadron susceptible to cyber-attacks and infiltration that could jeopardize the agency's mission and the integrity of classified information, and

According to OSC, "[REDACTED] disclosed that EADS IT officials, including [Subject], have been aware of serious security shortcomings within the EADS unit's mission-critical IT systems since before January 2020, but have chosen not to rectify these vulnerabilities. [REDACTED] also alleged that many systems lack required documentation, redundancy, and data backups, including servers that store classified, mission-critical data, and systems that control employees' network access. Management, including [Subject], is aware that classified information is not being backed up, but has chosen not to implement readily-available solutions, leaving mission critical systems and information vulnerable to complete loss as well as outside threats. [REDACTED] further disclosed that [Subject], permitted the use of insecure Wi-Fi/"MiFi" and cellular communications, linked to insecure, external carriers and public networks, within secure, mission critical operational areas,

This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside Inspector General channels without prior approval of the Inspector General (DAF/IG) or designee

CUI

compromising the security of classified information in violation of agency policy. [Subject], also permitted the unit's performance monitoring software license to lapse, preventing staff from early detection and identification of potential areas of concern, such as security breaches and network connectivity loss."

[Subject] has grossly mismanaged EADS resources, including failing to track agency assets containing classified information, failing to provide support for existing IT systems, and directing the improper disposition of excess government property in violation of agency policy.

According to OSC, "[REDACTED] further alleged that [Subject] has not ensured proper asset tracking, leading to the unsecured storage and disposal of classified IT hardware and the destruction of usable, unclassified hardware still under warranty.

According to [REDACTED], [Subject] also encouraged employees to undermine the effectiveness of a system called SecureView by refusing to support the system, which the head of the EADS planning department deployed for mission-critical operations. As a result of the neglect and failure to provide support, the system ultimately degraded and could not be used. [REDACTED] alleged that [Subject] also condoned the abandonment or destruction of more than \$50,000 worth of new, custom-made furniture that could not be used or returned. When [REDACTED] inquired about repurposing the furniture in February 2021, he was informed that the furniture was "trashed" in violation of 41 CFR § 102-36."

In its referral letter, OSC also noted, "that specific allegations and references to specific violations of law, rule, or regulation are not intended to be exclusive."

The OSC Referral Letter was forwarded for investigation through the Air Force General Counsel and the Secretary of the Air Force (SECAF). The SECAF's office forwarded the investigation to the Department of the Air Force Inspector General (DAF/IG) on July 6, 2021. On December 14, 2021, DAF/IG tasked an Investigating Officer to conduct an investigation into the above-referenced allegations as contained in the OSC Referral Letter. The delay in assigning the case to an IO was due to IO availability. Subsequently, a Technical Advisor from the Cyber Effects and Information Operations Division, Headquarters of the Air Force was identified to serve as a Subject Matter Expert (SME). In the course of the OSC investigation, the IO conducted an initial complaint analysis interview with [REDACTED] under oath on January 31, 2022. The investigation was conducted from 18 Dec 21 to 20 May 22 in Washington D.C.

Complainant stated that Subject has known about the shortfalls identified in the work center for a long time, prior to January 2020, because Complainant was told that Subject was previously the OIC of the communications work center. Complainant also suggested that Subject's negative influence/gross mismanagement prevented the correction of the identified deficiencies. The IO determined that the scope of the investigation would cover the time period that the Complainant was knowledgeable about and limited the scope of the inquiry specifically to Subject's actions since he was the focus of the complaint. Of note, a Unit Effectiveness Inspection (UEI) was completed on October 2020; the issues disclosed by the Complainant were not annotated as major concerns, and no major deficiencies were noted by the UEI. (Section III, Tab D (3.A), pgs. 5-18)

Complainant stated that the previous Flight Commander was his supervisor for the majority of his time from his date of hire, 16 Aug 20, to approximately 1 Mar 21 and stated, "just over 30 days

after [Subject] took over, um, I was terminated.” (Section III, Tab C (1), pg. 6, lines 5-6)

Complainant viewed the previous Flight Commander as supportive of his plans and did not fault him for any of the deficiencies. Complainant attributed the long-standing issues that he brought up in his complaint solely to Subject, despite the fact that the previous Flight Commander served in the position roughly eight months before Subject assumed the role. (Section III, Tab C (1), pg. 5, lines 16-19) The previous Flight Commander attested to the fact that he was the Director of the hiring Board that hired Complainant as SCOO IT lead to “inject leadership” within the SCOO. (Section III, Tab C (2), pg. 8, lines 19-21)

Complainant stated that he was hired as the IT Lead of the civilians and contractors within the work center. However, the exact nature of Complainant’s role as a supervisor was unclear. For example, while the previous Flight Commander confirmed that he had hired Complainant to provide leadership to the staff, a MFR dated 9 Mar 21 from the SCOO Section Chief stated that the Complainant “*did not have any tasking authority or any kind of management authority over your colleagues.*” (Section III, Tab D (1.E), para. 2) Another email from Subject stated that the others in the work center were his peers and he was not to demand work of them, however, he was referenced as the IT Lead Technician. (Section III, D (1.F), pg. 2) The previous Flight Commander did state that the leadership understood that Complainant would have a significant challenge transitioning from a corporate executive to being a Federal employee. (Section III, Tab C (2), pg. 10, lines 13-14) The previous Flight Commander noted that Complainant had expressed frustration with how “*slow*” things operated compared to a civilian company. (Section III, Tab C (2), pg. 11, lines 1-3) Complainant did not have the required certification upon initial hire, Security+, or TS/SCI clearance to work in the secured areas of the campus when he on-boarded with the unit. (Section III, Tab C (1), pg. 32, lines 19-25) Complainant worked for about two to three months at the Helpdesk with an Interim Secret clearance.

The previous Flight Commander testified that when Subject took over as the Officer in Charge (OIC) of the SCOO, there was a command directed initiative to “assign metrics” to the performance of the 224 SS. (Section III, Tab C (2), pg. 18, lines 12-24) He further stated that as a result of the directive, the priorities changed for SCOO from core functions to gathering data. Included in the core functions were systems upgrades mentioned on two separate occasions in emails from Complainant to Subject. The previous Flight Commander stated that as OIC, he prioritized “core responsibilities,” of the SCOO while he served as the Flight Commander and further testified that these core responsibilities were often overcome by “*other requirements that [were] trickling down.*” (Section III, Tab C (2), pg. 12, lines 2-13) The previous Flight Commander testified that the “*requirements trickling down*” made it difficult for an understaffed, and overstretched team to accomplish core functions given many personnel were working from home due to COVID and time constraints, although plans were devised to mitigate vulnerabilities. (Section III, Tab C (2), pg. 12, lines 7-13)

The Assistant Section Chief provided further insight on the difference in the previous Flight Commander’ leadership and Subject. The Assistant Section Chief stated that the previous Flight Commander was occupied with the missions of his other directorates and that Subject was more hands-on and prioritized the operational needs of EADS’ primary mission over the operational objectives of his own support section’s mission. (Section III, Tab C (3), pg. 75, 18-25) For example, the Assistant Section Chief found it difficult to update vulnerabilities found in the screen used by Ops Floor to view the weather, although an alternative screen could have been used while the system

This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside Inspector General channels without prior approval of the Inspector General (DAF/IG) or designee

CUI

was updated. Subject was characterized by the Assistant Section Chief as “handling fires” and “very directive.” (Section III, C (3), pg. 70, lines 1-17) While the previous Flight Commander was characterized as more diplomatic in his approach, the Assistant Section Chief testified that, *“he had to play things tactfully between multiple Work Centers.”* (Section III, C (3), pg. 69, line 17) When the SCOO Section Chief was asked how he would characterize Subject’s leadership style, he shared similar sentiments as expressed by the Assistant Section Chief. The SCOO Section Chief stated that Subject was *“really mission focused.”* (Section III, Tab C (5), pg. 9, line 3) The SCOO Section Chief stated that Subject was, *“making sure obviously ADS has all the support they need”* and that *“he takes everything very serious.”* (Section III, Tab C (5), pg. 9, line 3-4) The SCOO Section Chief noted that Subject was, *“not going to take something lightly. He's going to do his research, make sure everything is truthful and we're not just making just random allegations or complaining about subjects.”* (Section III, C (5), pg. 9, lines 5-7)

Complainant indicated in his clarification interview that all of the deficiencies he had pointed out in the email, were the areas that he perceived Subject should have been addressed more fully. (Section III, Tab D (1.D), pg. 5) In response to the noted deficiencies, Subject agreed, in part, with the analysis regarding the need for action. He then questioned the need to accomplish the network changes so quickly. Two of the systems discussed in the email were *“de-commissioned”* during or shortly after the termination of Complainant, SecureView and US ONLY Secure Internet Routing Protocol (SIPR). (Section III, C (5), pg. 31, lines 17-24) The Complainant indicated that both systems, despite the impending sunset of the system life cycle, were mission critical. (Section III, Tab D (1.D), pg. 5) However, both the Assistant Section Chief and the SCOO Section Chief testified that both systems had been de-commissioned.

An interview with the previous Flight Commander, revealed that the following issue was not supported by testimony or evidence:

“According to the Complainant, [Subject] also encouraged employees to undermine the effectiveness of a system called SecureView by refusing to support the system, which the head of the EADS planning department deployed for mission-critical operations. As a result of the neglect and failure to provide support, the system ultimately degraded and could not be used.” (Section III, Tab A (1), pg. 2)

SecureView. SecureView is a system comprised of hardware specifically designed to provide an encryption tunnel, allowed a single computer to host multiple guest virtual machines (VMs) running at different classification levels. (Section III, Tab D (4A), pg. 1) The SecureView system version 1.2, developed and distributed approximately seven to nine years prior by the Air Force Research Laboratory (AFRL) and a civilian defense company (AIS), accommodated the command element located in an unclassified building. (Section III, C(3), pg. 7, lines 21-25) According to the Assistant Section Chief, the unit received an initial accreditation of 17-20 machines of SecureView. (Section III, C (3), pg. 8, lines 4-12) The SecureView capability was developed for leadership to prevent the need to leave the building to access classified terminals. SecureView made access to classified material more easily accessible, however, the absence of the capability did not pose a mission threat according to the previous Flight Commander, *“Because there’s always the hardline gate, uh, SIPR terminal and [Non secure Internet Routing Protocol] NIPR terminal all over the place in the unit,”* meaning there were multiple ways to access classified information within the compound. (Section III, C(2), pg. 21, lines 11-12)

This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside Inspector General channels without prior approval of the Inspector General (DAF/IG) or designee

CUI

The previous Flight Commander also testified that Complainant's predecessor was "heavily involved" in the maintenance of the system. (Section III, C (2), pg. 22, lines 24-25) However, due to a loss of expertise and higher priorities, the system was not upgraded and essentially rendered "*unusable for a long period of time.*" (Section III, C (2), pg. 20, lines 1-7) The Assistant Section Chief further stated that, the [SecureView] system required a sustainment purchase because the Trusted Platform Module (TPM)¹ chips inside the systems "*didn't meet the new Air Force Standard.*" (Section III, Tab C (3), pg. 9, lines 7-15) The Assistant Section Chief further testified that, it was determined that the old equipment was too difficult to upgrade and the new systems too costly to acquire and maintain. The Assistant Section Chief stated, "*For the amount of money that was an annual requirement contact with AIS for support, the hardware updates, the maintenance, the actual back end infrastructure also went through a hardware, uh, upgrade, that just the amount of funds being produced didn't justify 15 client systems at our unit.*" (Section III, Tab C (3), pg. 10, lines 5-8)

AFI 17-1203, *Information Technology Asset Management*, defines full cost of ownership to include acquiring hardware, supplies, or services and other associated costs. The previous Flight Commander also testified that he had personally presented, "*pros and cons to the stakeholders*" between Dec 20 and Jan 21. (Section III, Tab C (2), pg. 23, lines 12-16) According to the previous Flight Commander's testimony, the stakeholders agreed that the SecureView system would no longer be used. (Section III, Tab C (2), pg. 23, lines 18-21) The decision to terminate the sustainment and maintenance of the fielded equipment pre-dated Subject and the decision was not isolated to Subject. Based on the preponderance of evidence, the IO concluded that no violation of rule, law or regulation occurred that could be attributed to Subject. Given the date of the initial fielding on or about 2012, the hardware was outdated and could be disposed of in accordance with AFI 17-1203 and the system classification.

Performance Monitoring Software. Complainant attributed the unit's lack of performance monitoring software to Subject but also stated that he "*didn't personally witness this, this is what I was told by [the Assistant Section Chief].*" (Section III, C (1), pg. 54, lines 18-19) Complainant perceived that the lack of performance monitoring software contributed to the vulnerability of the organization. Complainant indicated that, "*I didn't find that out until much, much, much later. But he said, [Subject] did not want to spend the money to renew the software license, and so when the software license expired, it stopped working, and so we basically, uh, got rid of the equipment, so now we have no capability to monitor.*" (Section III, C (1), pg. 55, lines 11-14) Complainant described the need and stated, "*you would typically have some software that would monitor all your key critical equipment, as well as your telecommunications, and network infrastructure, uh, so that if an item failed -- and that could be, you know, let's say a, a network link to a remote site, or it could be a server, or, you know, a hard drive, or something like that, if it, if it was critical, you monitored it.*" (Section III, C (1), pg. 54, lines 20-24)

The Assistant Section Chief stated that the SCOO actually maintained 3-4 physical servers. (Section III, Tab C (3), pg. 55, lines 3-5) The remaining servers, are managed by the NOSC and

¹ Trusted Platform Module- cryptographic module that enhances computer security and privacy. Protecting data through encryption and decryption, protecting authentication credentials, and proving which software is running on a system are basic functionalities associated with computer security. Retrieved from <https://www.microsoft.com>, 1 Mar 2022.

maintained by the SCOO depending on the level of service required. (Section III, Tab C (3), pg. 54, lines 3-5) Complainant further noted that the Operations would notify the SCOO of an outage. (Section III, C (1), pg. 55, lines 20-21) When the IO asked the Section Chief about the operation of the 224 SS, he indicated a specific protocol to address incidents or outages that involved a 24 hours per day/7 days a week Cyber Watch and on-call technician support specifically to quickly identify and address outages. (Section III, C (5), pg. 30, lines 12-21) When the IO asked the Equipment Control Officer about network monitoring software, she replied that they use Assured Compliance Assessment Solution “ACAS” to scan the network for vulnerabilities. (Section III, C (4), pg. 26, lines 16-23) Additionally, it was noted that updates are pushed to clients and monitored through Active Directory. (Section III, C (4), pg. 27, lines 19-21) In accordance with AFI 17-1203- para. 3.4.2.8., software license purchases are facilitated by the Unit Asset License Manager (UALM), therefore, would not be the sole responsibility of Subject. While Complainant indicated a specific type of performance monitoring software would improve mission efficiency, the unit was still able to monitor the network through continuous monitoring, business rules and other applications. There was no clear indication of a violation of rule, law or regulation.

Portable Electronic Devices (PED). Complainant alleged that Subject permitted the use of insecure Wi-Fi/“MiFi” and cellular communications, linked to insecure, external carriers and public networks, within secure, mission critical operational areas, compromising the security of classified information in violation of agency policy. Complainant implied that Subject failed to implement emission security countermeasures for “portable electronic devices” (PEDs) in close proximity to National Security Systems in violation of AFSSI 7702, *Emissions Security* and AFMAN 17-1301_AFGM 19-01, *Computer Security*. Complainant explained that the Information Assurance expressed non-support of the idea without a local policy and risk mitigation. (Section III, C (1), pg. 52, lines 1-5) Complainant testified to the fact that a policy was implemented and members of the leadership provided input into the policy. According to Complainant, the mitigation procedures included an approval through the chain of command, isolation to the communal breakroom, cell phones must be turned off upon entry into the building as well as a device detection protocol was put in place. (Section III, C (1), pg. 52, lines 9-15) Complainant stated that there were a number of breaches and “no one would do anything.” Based on hearsay, Complainant alleged that Subject ordered the device detection system turned off because the alarm was close to his office. (Section III, C (1), pg. 54, lines 1-5)

The IO found that proximity to classified systems is addressed in the emission security AFI and specifically addresses cellular phone use. In accordance with EMSEC 3.4.4, when a cellular telephone is used as an operational necessity, separate it 5 meters from RED equipment. When the cellular telephone is a personal asset, disable the unit from receiving calls or separate it 10 meters from RED processors. Cellular telephones are excluded from operating within 10 meters of the classified information processing area when the facility is located outside the United States. Also based on EMSEC policy, the use of cellular phones is permitted for short amounts of time given that the cellular phone in use is a specific distance from classified materials. The mere presence of a cellular phone in a building containing classified materials, is not a violation of rule, law, regulation or policy. Another mitigation procedure described by both the previous Flight Commander and the Assistant Section Chief was the use of a restrictive hallway or corridor to the breakroom. Both witnesses testified that the path to the breakroom was isolated from classified materials.

When asked by the IO who was responsible for the establishment of the policies, the previous Flight Commander stated that the Commander had an assigned Information Protection Officer, who worked with internal Security Forces to determine the mitigation procedures. (Section III, Tab C (2), pg. 36, lines 8-14) EMSEC procedures were noted as a deficiency on the 224 ADG Unit Effectiveness Inspection (UEI) conducted in October 2020. In an effort to address challenges detailed in the UEI, the command highlighted the fact that four civilian employees were hired recently. The previous Flight Commander denied knowledge of any incidents concerning PEDs. The electronic detection devices were on order and “*took a while before the equipment actually showed up,*” to his recollection. (Section III, Tab C (2), pg. 16, lines 1-3) Based on the fact that Subject was not the Responsible Managing Official for Information Protection, Security, or an authorizing official of the policy, the IO determined that the preponderance of evidence does not support any violation of law, regulation or policy on this matter. The unit Commander assumed the risk when he instituted the local policy enforced by the Information Protection officer and Security Forces.

The Assistant Section Chief recalled instances when Security Forces asked violators to remove their phones and recalled a registration requirement for devices in use. When asked if there was a time that the devices were turned off, the Section Chief recalled a time when the Operations Group requested the device nearest the Ops room floor be turned off because it was triggered at the cell phone turn-in station. (Section III, C (5), pg 16, lines 22-24) The Assistant Section Chief attested to the fact that the Communications Support team did not control the devices. Those devices were controlled by Security Forces. (Section III, Tab C (3), pg. 12, lines 10-14) There was no credible evidence presented to support the allegation that Subject violated a rule, law, regulation or policy.

Furniture. According to Complainant, Subject, “*condoned the abandonment or destruction of more than \$50,000 worth of new, custom-made furniture that could not be used or returned.*” (Section III, Tab A (1), pg. 2) Complainant alleged that the SCOO Section Chief and Subject told him the furniture was “trashed”. (Section III, C (1), pg. 67, lines 10-21) When the IO inquired about \$50,000 worth of custom-made furniture, the SCOO Section Chief denied anyone disposed of the furniture. The SCOO Section Chief made it clear that the furniture was delivered. He stated that it did take a long time to receive. Once received, part of the furniture was put in use in another building, not the original planned location. The other part of the furniture was being stored in a dedicated connex in the parking lot. The IO determined that no violation of rule, law or regulation occurred.

SIPR Data Backups. Complainant alleged that data was not being backed up on the secure network and recounted an event where he relayed the urgency to the Commander,

“Um, I, I can tell you. I can tell you [Commander], himself, the Commander, uh, could probably at, at least attest to the fact that, uh, at, at one of his tours of the work centers, um, him and I had the conversation about the fact that we weren’t backing up, uh, classified data, and, and he kind of came unglued and said, what, and I said yeah, I mean, uh, I, I assume that’s important. And he was like, you’re damn right it’s important, that needs to be resolved immediately. And, you know, he said that in front of everybody in the work center. And, you know, I took that to mean that, okay, we need to jump on this. We did. Um, but then that got countermanded, uh, you know, about two months later, uh, when [Subject] took over.”
(Section III, C.1, pg. 76, lines 7-17)

Complainant reflected that the discussion with the Commander occurred almost two months prior to the Subject's assumption as Flight Commander, on or about January 2021. When the IO asked the previous Flight Commander who was designated to execute the secure backups, he stated that the task was "*collective*" and that no one person was designated to execute the tasks. (Section III, Tab C(2), pg. 24, lines 22-25) The previous Flight Commander also mentioned ordering an encrypted drive to store the data. A Complainant- provided MFR from the SCOO Section Chief to Complainant issued in March indicated that Complainant was tasked with ownership of the SIPR backup issue along with a significant milestone indicated to brief the project plan. (Section III, Tab D (1.E), pg. 1 para. 4) The SCOO Section Chief stated, "*SIPR backup is a significant threat to our mission continuity. Please own the resolution of this shortfall in its entirety.*" (Section III, Tab D (1.E), pg. 1 para. 4) When the IO asked the Assistant Section Chief who was tasked with the SIPR data backups, he testified that Complainant was solely tasked to address the issues with SIPR and stated, "*As I was divided in my tasks, and everything was handed over to [REDACTED].*" (Section III, Tab C (3), pg. 19, line 4) The Assistant Section Chief further attributed Complainant's inability to complete a project designated to him as one of the reasons for his termination in his testimony stating, "*when they tried to pull back everything that he was doing and task him with one task item, do the SIPRnet backup, and it took a month, and he just kind of didn't produce anything.*" (Section III, C.3, pg. 78, lines 8-10)

The Assistant Section Chief further described a migration from US-ONLY SIPR to a Coalition network that allowed both US and CAN to access SIPR through the same network. This project resulted in a decreased reliance on the US ONLY SIPR. (Section III, Tab C (3), pg. 18, lines 8-16) The reduced services resulted in fewer clients requiring SIPR data backups and testified that the team, "*took a little extra time to not worry so much because there was very few users left utilizing the older network.*" (Section III, Tab C (3), pg. 18, lines 15-16) Additionally, the Assistant Section Chief stated that NORAD backed up their own data and that backups for the US ONLY SIPR and stated that what was, "*maintained and managed on our U.S. only network was a full copy,*" during the migration from the old SIPR system to the new one. (Section III, Tab C (3), pg. 23, line 6) The Assistant Section Chief acknowledged that due to COVID and manning shortage during the period of Aug 2020 to Apr 2021, the frequency of the completing SIPR backups was done on a monthly basis versus the weekly requirement. (Section III, Tab C (3), pg. 18, lines 2-6) When asked if the backups were completed, the Assistant Section Chief answered in the affirmative and testified that, "*we had to identify U.S. only, SIPRnet secret side backup, and get them done more often.*" (Section III, C (3), pg. 16, 12-13)

Complainant mentioned that Subject would mention that the, "*WADS can take over, if we go down.*" (Section III, C (1), pg. 73, line 6) When the IO asked what he meant, Complainant stated that it meant the Western Air Defense Sector (WADS) could assume the EADS mission in the event of a failure. When the IO asked the Assistant Section Chief if he had heard this statement without mentioning Subject, the Assistant Section Chief replied in a matter of fact tone, "*So, that's not my system to worry, that's, that is the mission set for EADS, and if my stuff drops, it's not, you know, going to effect the Eastern Air Defense Sector mission.*" (Section III, Tab C (3), pg. 57, lines 20-22) He also explained that EADS and WADS have the same capability in their air defense mission and can "*In the event that one of these two sectors was blown up by a missile, the other Air Defense Sector can pick up that mission and still see the entire United States scope,*" if the EADS capabilities fail. (Section III, Tab C (3), pg. 57 lines 17-19) The WADS is the logical backup to mission critical

systems housed at the Griffiss campus. The Assistant Section Chief testified that the SCOO did not monitor the communications assets associated with critical “mission systems.”

Cyber Mission Systems (SCP) was charged with direct support to critical “mission systems,” while SCOO provided support to ancillary systems (i.e. computers, printers, functional servers). (Section III, Tab C (3), pg. 3. Lines 15-19) Additionally, a team of Cyber Defense Officers performed a continuous monitoring function, twenty-four hours a day and seven days a week, alerting relevant teams of significant communications outages. (Section III, Tab C (5), pg. 30, lines 12-21)

Given the preponderance of the evidence, the IO determined that Subject took several steps to remedy the deficiency with countermeasures once the risk was assessed. The evidence and the testimony did not support the allegation that a rule, law, regulation or policy was violated by the Subject.

Vulnerabilities. Two systems were identified by the Complainant as systems with vulnerabilities: the Remote Authentication Dial-In User Service (RADIUS)² and Patriot Excalibur (PEX)³ servers. (Section III, Tab D (1.D), pg. 4, para (d)) Of the two systems, only the PEX server was reported to have vulnerabilities identified through a Notice to Airman (NOTAM).⁴ When Complainant asked Subject why certain vulnerabilities should not be addressed, he stated that, *“he basically said [Vulnerability Manager] had been here longer than you and if [Vulnerability Manager] saying it’s not important, then it’s not important, ignore it.”* (Section III, C (1), pg. 38, lines 6-7) While two witness statements provided an overview of the vulnerability management program and its challenges, it was unclear, at the time, if Subject “ignored” the vulnerabilities identified in the PEX servers.

Complainant attributed identified single points of failure in the network and a lack of redundancy in the RADIUS servers, to Subject. Complainant alleged that Subject negatively influenced and grossly mismanaged the assets and stated, *“Those capabilities were allowed to be, uh, ignored, and they were not repaired, and they were not addressed,”* citing two Remote Authentication Dial-In User Service (RADIUS) server incidents as an example. (Section III, C (1), pg. 72, lines 12-14) One incident occurred before Complainant was hired and the other occurred while he was employed with 224 SPTS/SCOO. A server containing the RADIUS network protocol, otherwise termed a RADIUS server, failed. The first failure resulted in approximately three weeks downtime, according to Complainant. Complainant recalled that the unit waited for specific

² Remote Authentication Dial-In User Service (RADIUS) is defined as a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service. Retrieved from <https://www.docs.microsoft.com>, 1 Mar 22.

³ Patriot Excalibur (PEX), developed by Air Force Mobility Command (AFMC) at Eglin Air Force Base (AFB), is a unit-level software tool that coordinates the activities of military flying, Intelligence, air operations center, para-rescue, aero-medical, tactical air control, intercontinental ballistic missile (ICBM), and security forces squadrons in the areas of Scheduling, Aircraft Maintenance, Qualification/Continuation training, and Standards/Evaluation. Retrieved from Patriot Excalibur (PEX), <https://www.my.af.mil>, 12 Apr 22.

⁴ A Notice to Air Missions (NOTAM) is a notice containing information essential to personnel concerned with flight operations but not known far enough in advance to be publicized by other means. It states the abnormal status of a component of the National Airspace System (NAS) – not the normal status. Retrieved from *Notice to Air Missions*, <https://www.faa.gov>, 12 Mar 22.

This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside Inspector General channels without prior approval of the Inspector General (DAF/IG) or designee

Technicians to provide external support. (Section III, C (1), pg. 72, lines 23-24) In an effort to avoid similar downtime, Complainant devised a plan to repair the outage. Complainant stated that he consulted the Section Chief, who supported his solution to take an unused piece of equipment from the rack to repair the RADIUS server and, “*Then we got in trouble with [Subject].*” (Section III, C (1), pg. 23, line 14)

Complainant alleged that the lack of proper documentation prevented him from knowing that the equipment was “*supposed to have been turned in three years ago,*” a fact he was unaware of until he was told by Subject at the time of the incident. (Section III, C (1), pg. 23, line 14-17) Complainant alleged that Subject failed to track assets appropriately and the IO recommended investigation. In accordance with AFI 17-1203, *Information Technology Asset Management*, para. 2.4.2.1-2 Controlled Inventory IT assets are any IT hardware with persistent storage (e.g., laptop, desktop, server, tablet, smartphone, external hard drive, and thumb drive) and must be accounted for in Defense Property Accountability System (DPAS). The Accountable Property Records (APR) are maintained by the Equipment Control Officer (ECO). Subject is not the designated ECO, however, he supervised the ECO. Both the Equipment Control Officer and the Assistant Section Chief reiterated the equipment turn-in process. The ECO noted that there had been a “moratorium” on inventorying assets since the pandemic began. (Section III, C (4), pg. 11, lines 19-20) The ECO also noted that equipment that is taken off the network and is subsequently used as a “spare,” may not necessarily be brought to the ECO for turn-in and subsequently removed or turned in through DPAS; it could be re-designated with an additional “six characters” as a description. (Section III, C (4), pg. 23, lines 9-23) AFI 17-1203 Table 2.2, provides equipment life spans by type.

While the preponderance of the evidence gathered to date did not support further inquiry or investigation into Subject as the primary Responsible Management Official, additional details on Subject’s influence were required in order to provide more clarity to the specific equipment, incidents and preponderance of evidence to determine if a rule, law or regulation was violated.

When the IO asked Complainant about the nature of Complainant’s allegations, Complainant stated, “*There is no documentation,*” when discussing the incident to repair a RAID [IUS] server. (Section III, C (1), pg. 40, line 17) Complainant later referenced in testimony, “*CSIRs⁵ drawings were out of date and were no longer valid*” to identify the equipment to use, negating the implication that no schematics existed at all. (Section III, C (1), pg. 24, line 19) In accordance with AFI 17-101 para 3.12., *Cyberspace, Risk Management Framework (RMF) for Air Force Information Technology (AFIT)*, the Information System Security Manager (ISSM) is the primary cybersecurity technical advisor to the Authorizing Official, Program Manager, and Information Security Officer. For base enclaves, the ISSM manages the installation cybersecurity program, typically as a function of the Wing Cybersecurity Office. AFI 17-101 para. 3.12.3., further states that the ISSM ensures all AF IT cybersecurity-related documentation is current and accessible to properly authorized individuals.

Initially, it was unclear if the network access this RADIUS server provided was TEMPEST-certified equipment, classified, or provided access to mission critical systems. According to testimony provided by the Assistant Section Chief, two servers (Classified and Unclassified) existed

⁵ CSIR- Communications and Information Systems Installation Records is master CSIR file for communications and information systems or facilities. Retrieved from *Communications and Information Base-Level Planning and Implementation*, <https://apps.dtic.mil>, 27 Apr 22.

This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside Inspector General channels without prior approval of the Inspector General (DAF/IG) or designee

to provide additional network protection, however, he noted that the servers were “critical”. A manual solution would allow access to the connecting services in the event of a failure. The Assistant Section Chief stated, “*Radius absolutely can impact our network, but it is no means an end-all, be-all. Our work-around would be to manually configure the switch to manually allow workstations back in.*” (Section III, C (3), pg. 47, lines 22-25)

Lastly, during a discussion on the allegation of improper classified drive disposal during the complainant's interview, the complainant disclosed that he was directed and complied with Subject's direction to throw away a classified drive without first completing the proper disposal actions. According to testimony provided by the Primary and Alternate Equipment Custodian Officers (ECO), classified drives undergo a process of removal from the housed equipment (i.e. server), are degaussed, re-marked with identifying stickers, and documented prior to disposal. Both witnesses denied a disclosure regarding a classified hard drive being “*thrown away without degaussing,*” “*misplaced,*” or even a rumor of such an occurrence. The Alternate ECO noted that such an occurrence equated to a security incident reportable to base Security Forces. Complainant stated that the only witness to the incident was an Airman who has since terminated service. With no witnesses to confirm this event other than Complainant's version of events, and in the interest of avoiding the perception of investigation Complainant, the IO elected to not pursue this matter further.

The standard of proof used in determining the finding for each allegation was the preponderance of the evidence, *i.e.*, was it more likely than not that the alleged violation occurred.

Pursuant to 5 U.S.C. 1213(c), an agency is afforded 60 days to complete the required report of investigation.

Pursuant to 5 U.S.C. § 1213(d), the Secretary's report to OSC is required to include, among other things, “a listing of any violation or apparent violation of any law, rule, or regulation.”

"The Secretary of the Air Force has sole responsibility for the function of The Inspector General of the Air Force (Title 10, United States Code, Section 8014). When directed by the Secretary of the Air Force or the Chief of Staff of the Air Force, The Inspector General of the Air Force (SAF/IG) has the authority to inquire into and report upon the discipline, efficiency, and economy of the Air Force and performs any other duties prescribed by the Secretary or the Chief of Staff. (Title 10, United States Code, Section 9020.) Pursuant to AFI 90-301, *Inspector General Complaints Resolution*, authority to investigate IG complaints within the Air Force flows from SAF/IG to IG offices at all organizational levels."

Section II, Tab C – Findings of Fact, Analysis, Conclusion(s), and Recommendations.

CHRONOLOGY:

DATE	EVENT	SOURCE
10 Mar 20	Global pandemic declared. Government agencies limit in-person work schedules to mission essential	(Section III, Tab D (12A), pg.(s) 1-4)
25 May-10 Jul	224 SS Vertical Inspection conducted by EADS/IG	(Section III, Tab

This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside Inspector General channels without prior approval of the Inspector General (DAF/IG) or designee
CUI

20		D (3.B), pgs. 1-20)
16 Aug 20	Complainant is hired as an IT Specialist (Network) in the 224 SPTS.	(Section III, Tab D (1.I), pg. 1)
15-20 Oct 20	Unit Effectiveness Inspection (UEI) Report for 224 ADG	(Section III, Tab D, (3.A), pgs. 1-22)
19 Nov 20	Group Policy Updates not registering on computers with automatic updates. Complainant raised concern that the updates would have to be completed manually, a potential server issue.	(Section III, Tab D, (1.K), pg. 9)
3 Dec 20	Complainant awarded Civilian of the Quarter award.	(Section III, Tab D (1.A), pg. 2)
O/a 01 Jan 21	Complainant ordered to conduct classified backups after notifying the Commander of the issue while on a worksite tour.	(Section III, Tab C (1), pg. 76, lines 7-12)
O/a 01 Jan 21	Complainant completed one backup and the backups did not continue.	(Section III, Tab C (1), pg.25, lines 21-25)
O/a 01 Jan 21	Complainant became certified in Security+ and received TS/SCI clearance. Complainant granted Administrative rights and granted access to more secure areas. The SCOO Section Chief testified that Complainant received his Administrative Rights closer to January.	(Section III, Tab C (1), pg. 7, lines 6-8); (Section III, Tab C (5), pg. 10, lines 17-19)
O/a 01 Jan 21	Subject re-assumes a role as the OIC of the communications work center. Subject was dual-hatted as the Assistant Director of Operations (ADO).	(Section III, Tab C (5), pg. 7, ln. 21)
27 Jan 21	(PC) Complainant emailed Subject regarding meeting and metrics. Complainant documented the feasibility of the metrics given the allocated manpower. Complainant discussed reprioritizing in order to embrace the plan developed by Complainant and the Assistant Section Chief.	(Section III, Tab D (1.B), pg.1)
O/a Feb-Mar 21	Complainant alleged Subject improperly disposed of government property (custom furniture). Complainant alleged that he was assigned a project to accommodate more people in the work center. When it was determined that the work center could not be successfully upgraded to accommodate the requirements without a significant increase to the time and budget, the project was cancelled. Complainant awaited the furniture delivery scheduled to arrive two months prior. When	(Section III, Tab C (1), pg. 67, lines 10-21); (Section III, Tab C (1), pg. 66, lines 2-3)

	Complainant inquired about the furniture, he was told by Subject, the furniture was “trashed”. His interpretation of trashed meant it was put in the dumpster as opposed to being re-allocated to another government office or properly disposed of according to the law.	
O/a Feb-Mar 21	Complainant alleged that Subject failed to track unclassified and classified systems still under warranty, ordering the improper disposal of equipment under warranty. Complainant recalled an incident when he identified equipment that was erroneously discarded in the dumpster behind the building. When he asked Subject about it, he stated that it must have been thrown out by mistake. Complainant stated that Subject still told him to discard the equipment despite being under warranty.	(Section III, Tab C (1), pg. 61, lines 1-8)
01 Mar 21	Complainant provided Subject a DRAFT list of un-prioritized core tasks or projects with categories (Minor, Moderate, and Major) and impacts to a specific enclave (SIPR, NNC, All, NIPR).	(Section III, Tab D (1.C), pgs. 1-3)
01 Mar 21	Complainant responded to a question by Subject with an email that explained several deficiencies he defined as a "soliloquy" and gave his perspective on the priority actions. Subject responded and noted the "desperation" to the tone of the email and questioned whether Complainant had a "white hot" personality type. Complainant posited that he “did not understand what was truly important at EADS”.	(Section III, Tab D (1.D), pgs. 1-11)
09 Mar 21	Complainant issued an MFR from the SCOO Section Chief regarding Complainant's duties and responsibilities including a non-supervisory role for civilians in SCOO and one priority project following email on 2 Mar 21 to Subject. The MFR addressed concern over SIPR issue and assigned responsibility to Complainant to, "own all aspects of this effort" and identifies two significant calendar dates for the Complainant.	(Section III, Tab D (1.E), pg. 1.2-1.4)
15-31 Mar 21	Complainant finds a classified hard drive in an unclassified area. Complainant alleged that Subject instructed Complainant to “get rid of it” which Complainant interpreted to mean throw the classified drive in the dumpster.	(Section III, Tab C (1), pg. 69, lines 18-22)
15-31 Mar 21	Cell phones and MiFi/Wi-Fi use near classified systems.	(Section III, Tab C (1), pg. 54, ln. 10)
16 Mar 21	Suspense for EC-VoIP rollout; Complainant charged with operational checks.	(Section III, Tab D (1.E), pg.1.3)

17 Mar 21	Subject issued performance feedback to Complainant that indicated performance issues stemmed from Complainant abdicating ownership and an aggressive leadership style versus a cooperative one.	(Section III, Tab D (1.F), pg. 1.1)
19 Mar 21	Email sent from Human Resources, NYANG confirming Complainant made a "hostile work environment" complaint against "supervisor."	(Section III, Tab D (1.G), pg. 1)
26 Mar 21	Date specified in MFR for Complainant to brief the SIPR Way Ahead project plan in order to, "own all aspects of this effort."	(Section III, Tab D (1.E), pg. 1.4)
29 Mar 21	Email sent from Complainant containing an apology to the Subject for inconveniencing the squadron with interviews of "45" people. The email further explains failure to certify for Sec+ earlier and discussed the "training" recommendations/solutions. Complainant admits that others in the squadron told him to "stay in his lane."	(Section III, Tab D (1.H), pg. 1)
30 May 21	Letter of termination drafted and issued through Human Resources.	(Section III, Tab D (1.I), pg. 1)
02 Apr 21	Complainant terminated from position with EADS due to "conduct and performance."	(Section III, Tab D (1.I), pg. 1)
02 Apr 21	Litigation hold drafted addressed to Commander on behalf of the Complainant and sent to Primary Vulnerabilities Manager, Flight Chief, Subject, and Vice Commander.	(Section III, Tab D (1.J), pg. 1)

ALLEGATION 1. Between 27 January 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, failed to implement countermeasures to the Patriot Excalibur (PEX) servers, to mitigate “critical or high risk” vulnerabilities identified as Tier I in violation of AFI 17-130 *Cybersecurity Program Management*.

STANDARDS.

AFI 17-130 Cybersecurity Program Management, 13 Feb 20.

1.3. The cybersecurity program provides: Authorizing Officials (AOs), Information System Owners, Program Managers, Information System Security Managers, mission owners, and authorized users a way to balance the confidentiality, integrity, availability, and non-repudiation of Air Force information with the threats, vulnerabilities, and risk to the IT’s capabilities. This balance provides a way for all stakeholders to accept a level of risk while maintaining the capability for the mission. (Section III, Tab D (6.A), pg. 4)

2.9. Information System Owner (ISO) or Program Manager of AF IT. Responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. This includes traditional acquisition category programs and non-traditional acquisition category programs. The ISO or Program Manager shall:

2.9.1. Plan and budget for security control implementation, assessment, and sustainment throughout the system life cycle, including timely and effective configuration and vulnerability management. (Section III, Tab D (6.A), pg. 6)

2.10. Information System Security Manager (ISSM). Responsible for the IT's cybersecurity program within a program, organization, information system, or enclave. (Section III, Tab D (6.A), pg. 6)

2.10.3. Ensure implementation of IT security measures and procedures, including reporting incidents to the Authoring Official and appropriate reporting chains and coordinating system-level responses to unauthorized disclosures. (Section III, Tab D (6.A), pg. 6)

AFI 17-101, Risk Management Framework (RMF) For Air Force Information Technology (IT), 6 Feb 20.

1.1.1. The RMF incorporates strategy, policy, awareness/training, assessment, continuous monitoring, authorization, implementation, and remediation. (Section III, Tab D (6B), pg. 5)

Figure 1.1. Air Force IT Categories. (*Reference Enclaves*) (Section III, Tab D (6B), pg. 5)

1.3.2. The RMF ensures AF IT assets are assessed for cybersecurity risk. Discovered weaknesses are documented in a **plan of action and milestones (POA&M) to mitigate residual risk**. An AO, identified at Table 3.1, who is supported by an RMF team, accepts the risk for his/her area of responsibility, in accordance with DoDI 8510.01, and the Air Force RMF Knowledge Service. (Section III, Tab D (6B), pg. 6)

3.3. Authorizing Official (AO). The AO is the official with the authority and responsibility for **accepting risk for an IT system**. With the exception of **unmitigated** "Very High" and "High" risk, (see Terms) the AO balances the level of risk for a system with mission requirements. The AO is the only person with authority to grant authorization decisions within their area of responsibility. **All AOs have the flexibility in augmenting, executing, and implementing RMF for systems in their AOR.** (Section III, Tab D (6B), pg. 9)

3.12.6. Continuously monitors the IT and environment for security-relevant events, assess proposed configuration changes for potential impact to the cybersecurity posture, and assess

This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside Inspector General channels without prior approval of the Inspector General (DAF/IG) or designee

CUI

the quality of security controls implementation against performance indicators. (Section III, Tab D (6B), pg. 15)

4.9.2. The objective of an **Information Security Continuous Monitoring (ISCM)** program is to determine if the complete set of planned, required, and deployed security controls within a system or inherited by the system continue to be effective over time in light of inevitable changes. (Section III, Tab D (6B), pg. 23)

4.9.4. All implemented security controls, including management and operational controls, must be regularly assessed for effectiveness, even if monitoring them is not easily automated. (Section III, Tab D (6B), pg. 23)

REVIEW OF FACTS, PERTINENT TESTIMONY AND DOCUMENTATION.

- When Complainant was asked which law or regulation the Subject violated, he testified that, *“Well, I don’t know that I would say, um, that anything he did while I was there, um, had an immediate impact on the mission one way or the other.”* (Section III, Tab C (1), pg. 71, lines 13-14)
- Complainant discussed the potential for exploitation of vulnerabilities and concluded, *“Um, you know, I -- I could say that there were a lot of things that were degraded because of his [Subject] directions, um, that shouldn’t have been degraded and that had he not issued directives not to do certain things, those things would have been restored to, um, fully operational status.”* (Section III, Tab C (1), pg. 71, lines 22-25)
- According to Complainant in an email addressed to the Subject, the PEX server had an, *“inability to accept critical OS patches.”* (Section III, Tab D (1.D), pg. 4 para (d.))
- Complainant also noted in an email addressed to Subject, *“SCOO only became aware of this issues because of a NOTAM requiring that SCOO install certain upgrades by October 2020.”* (Section III, Tab D (1.D), pg. 4 para (d.))
- Complainant wrote to Subject, *“When it was discovered compliance was impossible due to this problem, SCOO obtained a POAM⁶ to delay compliance. That POAM extended the deadline until February but interestingly, SCOO did not really pursue actions to comply with requirement until shortly before the deadline- thereby effectively wasting 90 days’ time. When SCOO once again failed to meet the extended deadline, another POAM was obtained to extend it 30 more days. Although our SMEs are now pursuing resolution options, doing so is still not their primary focus and it seems our backup plan for another compliance failure is another POAM request.”* (Section III, Tab D (1.D), pg. 4 para (d.))
- As stated by Complainant in the email regarding priorities to Subject, *“Factually,*

⁶ Plan of Action and Milestones (POA&M or ‘POAM’, as referred to by the Complainant) - a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of this POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems .Retrieved from *OMB Memorandum 02-01*, <https://georgewbush-whitehouse.archives.gov>, 14 Mar 22.

EADS is one minor failure away from a major catastrophe defined as: Prevent OPS the ability to use PEX for one week.” (Section III, Tab D (1.D), pg. 6, para. (c))

- The Assistant Section Chief provided a condensed explanation of the update process in testimony and stated, *“So, there’s a lot that does go on behind the scenes. So, we, we fall in line with a lot of that stuff. So, any outlying item, whether identified by our scans, we will manually patch or reboot, or rebuild, uh, it will maintain compliance as best we can.” (Section III, Tab C (3), pg. 42, lines 1-3)*
- When the IO asked the Assistant Flight Chief if he recalled a time when he had what one would consider a critical vulnerability he testified that, *“But critical CATI vulnerability rises to the top of our list, and it’s a giant Excel Spreadsheet that we can sort in the first sort that we do is the critical stuff. So, for instance, I said, Log4J⁷, I think, earlier, um, Log4J being a critical vulnerability that has actually come out, and it is worldwide, it is international.” (Section III, Tab C (3), pg. 42, lines 13-16.)*
- The Assistant Section Chief further detailed how the example vulnerability continued to be monitored by the vendor and stated, *“When that came out, that listed as critical, and so a patch exists, and it took a little bit of time for those vendors to patch. It’s actually still out there, and it is still being researched, and people are still, certain vendors are still finding that their Log4J vulnerability exists somewhere in their product, and then all of a sudden, that’s a CATI critical vulnerability that’s brand new to the Enterprise.” (Section III, Tab C (3), pg.42, lines 20-24)*
- The Assistant Section Chief further expounded on the example of a critical vulnerability addressed globally, *“Um, there are, that’s not to say that there isn’t a process for things that are super critical, uh, Log4J, for instance, when it came out, um, I have a website that will go to on the high side on SIPRnet, and it will give me, hey, this one is so critical, you’re going to patch it in three days. So, the average patching for most vulnerabilities is 74 days, minus the ones that come out that are orders and fragmented orders that say, do it faster.” (Section III, Tab C (3), pg. 43, lines 12-16)*
- To explain the priorities, the Assistant Section Chief stated, *“So, the whole Air Force has a great big giant vulnerability world that does exist, and we’re constantly, every day, into what we call ACT or it’s another acronym, that’s Affine Compliance Tracker. So, the Affine Compliance Tracker, is daily, even the stuff that’s supposed to be patched faster. It’s a priorities list, and if we don’t patch it, we get disabled, turned off, um, quarantined and in some instances, the Air Force will actually put our computers in a separate, uh, network grouping to where everything in and out is audited until it’s patched.” (Section III, Tab C (3), pg. 43, lines 18-24)*
- The Assistant Section Chief provided an explanation of the consequences if the unit does not pursue patching quickly and stated, *“Because we would basically get a loss of service, so me being the back shop, my users in my environment, so my 400 or so users, would suddenly just not have a computer and not know why. If we didn’t do what we do in the back shop, which is absolutely strike list patch according to a Time Compliant Network Order, a TCNO, or a Technical Order or everything that kind of comes from,*

⁷ Log4J- the Apache Software Foundation has released a security advisory to address a remote code execution vulnerability (CVE-2021-44228) affecting Log4j versions 2.0-beta9 to 2.14.1. A remote attacker could exploit this vulnerability to take control of an affected system. Log4j is an open-source, Java-based logging utility widely used by enterprise applications and cloud services. Retrieved from *Apache Releases Log4j Version 2.15.0 to Address Critical RCE Vulnerability under Exploitation*, <https://www.cisa.gov>, 14 Mar 22.

uh, AF Cyber, on up into, um, Cyber con or com, sorry, Air Force..." (Section III, Tab C (3), pg.44, lines 22-25)

- The Assistant Section Chief described his urgency to patch critical vulnerabilities, *"Cyber Command, um, so it's a big entity that pushes this down to every wing site as wide as it goes and speeds all their stuff up and creates the whole tracking process, um, and if we can't patch, it's identified early, um, what we call POAM, um, what it's called, but we - but we seldomly use it, which makes me feel that I can't patch it in three days, but we'll patch it in ten, um, we seldomly use that arena, but. Yeah, a whole program associated to it, and these are Technical Orders. So, they're told to us to be done, or else there are consequences."* (Section III, Tab C (3), pg. 45, lines 1-10)
- When the IO asked the ECO how involved the IT Lead was in vulnerability management, *"So, when we started to -- you know, we were doing the vulnerability management, we would explain to him, and when I say we, I'm talking [Assistant Section Chief] and myself, to explain to him what actually needed to be done with the vulnerability management as far as scans, and remediations, and where we get the numbers for, you know, the software, and things like that. And, granted, that had to be done on two different networks. And, so, he -- I think because -- there was so -- there's just so much stuff, I don't know, maybe he was overwhelmed with everything that was going on, so we were -- you know, we were telling him, we were showing him, and he just wasn't -- I don't know if he just wasn't understanding what we were saying, or he wasn't really listening."* (Section III, Tab C (4), pg. 13, lines 13-23)
- When the IO asked about updates that did not meet the intended milestone date, the ECO testified about the difficulty in the PEX server updates and stated, *"And normally we, you know, tried every troubleshooting tool that we could to get it to take the updates."* (Section III, Tab C (4), pg. 28, line 19-20)
- The ECO continued to explain the previous comment and testified, *"So, we go -- once a week you go in and you, you know, kick off the updates on these servers, and they are set in called Active Directory, which is a, you know, directory of everything."* (Section III, Tab C (4), pg. 27, lines 19-21)
- When the IO asked the ECO if there was a time when the unit received a critical update, or a Tier I update that could not be accomplished by the milestone date, the witness answered in the affirmative and further explained the actions taken for the PEX server. The witness testified, *"We said, okay, we've got to put in a POA&M because this is a critical server for them even though, you know, it's not on their on the - you know, it's on the unclass[ified] network, but it's critical to them for their tracking and evaluation. So, we put in the POA&Ms to get that server -- you know, to give us time to work on that server because the last resort is to rebuild the whole thing."* (Section III, Tab C (4), pg. 29, lines 1-8)
- When the IO asked if the PO&AM extension was approved by the NOSC, the ECO testified, *"It actually went up to -- I think it was beyond the NOSC, the MCCC."*⁸ (Section III, Tab C (4), pg. 30, ln. 5)

⁸ Major Command Coordination Center- All major commands are required by headquarters Air Force to consolidate their network operations and systems under an MCCC as the single focal point for all network systems across the command. Retrieved from *Space command creates one focal point for networks*, <https://www.af.mil>, 26 Apr 22.

This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside Inspector General channels without prior approval of the Inspector General (DAF/IG) or designee

- When the IO asked if there was anything that could not be accomplished due to mission, the ECO testified that, *"We couldn't a hundred percent concentrate on the vulnerability management, which, you know, there is a lot of reporting, and information gathering that comes with that, and it's really a full-time job, and, so we really couldn't have -- dedicate somebody to just do that because we had so much -- so much other things to do."* (Section III, Tab C (4), pg. 11, lines 14-17)
- Subject testified to the main priority and stated, *"I mean the biggest ones we were working on was we were implementing the NORAD NORTHCOM different network; that was a huge undertaking because we were replacing our Air National Guard SIPR network with the NOSC."* (Section III, Tab C (8), pg. 7, lines 17-20)
- Subject explained that his time as the ADO and the Flight Commander were consumed with personnel issues, *"I wasn't directly involved with the technical work, I was mostly trying to solve the people problems in that Flight to try to get it back in order. And as I mentioned, there was -- it was clear that things weren't going well, that's why the original Flight Commander was relieved."* (Section III, Tab C (8), pg. 8, lines 14-17)
- Subject named the top five priorities and testified, *"It was like um, interaction with partners, um, training, um, focus on mission readiness, um, innovation; I can't remember the fifth one."* (Section III, Tab C (8), pg. 8, lines 21-22)
- When the IO asked about Subject's role in mitigating vulnerabilities he testified, *"I had no direct role or knowledge of what was going on with managing vulnerabilities. I was the SCO Flight Commander; SCOO is just one work center within the SCO Flight."* (Section III, Tab C (8), pg. 9, lines 13-14)
- Subject further stated, *"I didn't really get into much of the technical work and certainly the vulnerabilities at one server as part of one work center in that Flight, I helped correct knowledge or oversight and I'm not aware of any problems with it at that time."* (Section III, Tab C (8), pg. 9, lines 19-21)
- Subject attested to recollecting very little about the specifics of the PEX vulnerability, *"It was originally a physical server and they were working on switching it over to a um, virtual machine. I believe it was during that time period. That's the only memory I have of anything going on with the PEX Server."* (Section III, Tab C (8), pg. 10, lines 1-3)
- When asked if the PEX server would create a threat to mission systems, Subject testified, *"Not our Mission System, because those networks will then, they're totally separate, so even if it was compromised by some bad actor, they wouldn't have been able to get on to our Weapons System."* (Section III, Tab C (8), pg. 14, lines 12-14)
- When the IO asked in what capacity Subject signed the PO&AM, he denied signing as the ISSO or ISSM. (Section III, Tab C (8), pg. 12, lines 12-23)
- Subject sent a copy of the PO&AM for the PEX server, however, he identified that he was not the signatory, the Previous Flight Commander signed the document. (Section III, Tab D (13B), pg. 2)

ANALYSIS.

The IO examined Subject's role in the implementation of security controls and determined that Subject was not a technical subject matter expert or technician nor was he actively involved in day to day security control management. Complainant could not define

Subject's role or a specific violation, therefore, the standards of the RMF for an *Information System Owner* responsible for a *base enclave(s)* were applied. For base enclaves, the ISSM manages the installation cybersecurity program, typically as a function of the Wing Cybersecurity Office. Subject stated that the unit was a "GSU" or geographically separated unit. When asked to clarify, Subject stated, "*So, we're not on a base, we're just two buildings shrouded by a fence, um, and we're, you know, we're a group, we're not a wing.*" (Section III, Tab C (8), pg. 7, lines 7-8) There are seven processes⁹ that comprise the RMF, each key to vulnerability management and the overall Cyber Security Program. As defined by AFI 17-101, one of the processes within the framework is implementation, a process traditionally executed by a Technician and supervised by the chain of command. IAW AFI 17-101 para. 1.1.1, Subject was not the responsible for the hands-on implementation of the protocols, however, he was responsible for the continuous monitoring function that accompanies the implementation step within the RMF. Subject's role as a supervisor/ Information System Owner was to *assess* and *monitor*, two processes described as following the implementation phase of vulnerability management.

The PEX server was treated as critical, despite its operation on the NIPR network and the availability of the PEX application through a "*web-based app*". (Section III, Tab C (7), pg. 8, lines 16-19) The implementation of the security protocols through the automated process failed. The Assistant Section Chief provided an anecdote to indicate that Subject would, "*let the OPS floor and the Mission dictate the Support world, and so sometimes, the priorities are heavy-handed towards OPS rather than heavy-handed towards what we need to have accomplished,*" implying that PEX vulnerability management was not prioritized above operational needs. (Section III, Tab C (3), pg. 71, lines 21-23) Complainant implied that Subject negatively influenced the priorities. Complainant stated that Subject did not see things that, "*seemed to be the top priorities, addressed as a top priority*" of the Technicians but provided no supportive evidence beyond anecdotes. (Section III, Tab C (1), pg. 47, ln. 23) The ECO noted that the Operations personnel were "24/7" and it was challenging to work around their schedule. (Section III, Tab C (4), pg. 41, lines 12-15)

Subject was not involved with many of the day to day functions of vulnerability management because, as he testified, "*Usually, it's an automated process, so we only get involved with the ones that are manual, but maybe thousands, I don't know, like in a year, that are 'high-risk,' and um, and typically there's many layers of protection, not just you know, the one patch.*" (Section III, Tab C (8), pg. 17, lines 6-9) Subject testified that the allegations were written to, "*illicit the biggest emotional response.*" (Section III, Tab C (8), pg. 17, lines 2-3) Subject indicated that the actions noted were so routine that he could not recall the specifics regarding the vulnerabilities, only that the server was moved from being a "*physical server to becoming a virtual server.*" (Section III, Tab C (8), pg. 10, lines 1-3) It is more likely than not, Subject relied on the Technicians completing the work to advise on next steps in the process. Complainant perceived that the implementation was not timely, while noting actions taken to implement the security protocols. Other witnesses characterized Subject as focused on the air defense mission and stated, "*[Subject] was one of the most*

⁹ Risk Management Process includes seven steps: Prepare, Categorize, Select, Implement, Assess, Authorize and Monitor. Figure 4.1, AFI 17-101, *Risk Management Framework (RMF) For Air Force Information Technology (AFIT)*, 6 Feb 20.

This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside Inspector General channels without prior approval of the Inspector General (DAF/IG) or designee

logical and professional individuals that I've ever worked under. He always was absolutely unbiased in his approach to problems and decisions.” (Section III, Tab C (7), pg. 5, lines 3-4)

All six witnesses interviewed testified that personnel issues largely contributed to any inefficiencies in the workplace. The Assistant Section Chief stated, *“We had so many critical issues, it took a back seat, um, we only had so many bodies and then COVID, limited capacity as well, and we only had so much experience in the room, that there were too many jobs ahead of the SIPRnet backup solution.”* (Section III, Tab C (3), pg. 23, lines 21-24) The ECO indicated that vulnerability management was a *“full-time job”* without a person who could dedicate the time it required. (Section III, Tab C (4), pg. 11, lines 14-17) Complainant perceived the slow progression of the process a result of re-prioritization of effort directed by Subject, therefore, *“not the primary focus.”* (Section III, Tab D (1.D), pg. 4(d)) Subject testified that the PEX vulnerability, *“was nothing that rose within the level that I might -- anything greater than normal day-to-day business,”* and implied that it did not outweigh the priority of the ongoing SIPR project. (Section III, Tab C (8), pg. 20, lines 16-17) Subject further stated, *“SCOO was one work center in a Flight that was failing, that I had been sent down to fix, while still doing my ADO duties. There was a lot on my plate and I don't think that I would have gotten deeply involved with one technical problem, especially a common technical problem, as what is described here.”* (Section III, Tab C (8), pg. 20, 23-24)

The IT Lead received the required credentials to perform System Administration on or about January. The Flight Chief indicated that the expectation was that Complainant would be able to assist where the technical ability was lacking, however, testified that on the contrary, *“He didn't seem to have the technical knowledge of any of our systems, so he would reach out to our technicians for their input, and for their actual expertise for maintenance procedures, update procedures, anything that needed to be done on the system.”* (Section III, Tab C (7), pg. 20, lines 12-15) Subject stated in testimony that, one of the top 5 priorities for the time period was *“training.”* (Section III, Tab C (8), pg. 8, lines 21-22) Subject indicated that the server was initially configured using Program managed equipment. (Section III, Tab C (8), pg. 25, lines 4-7) However, Subject also testified that the IT Lead, who was also Complainant until his removal on 2 Apr 21, was partially responsibility for the implementation of the technical security protocols. Subject testified that, *“everything is my responsibility as the Flight Commander,”* however, he also stated that the responsibility was shared amongst the *“Technicians,”* the *“IT Lead,”* and the *“NCOIC.”* (Section III, Tab C (8), pg. 21, lines 7-13)

Contrary to the allegation, the evidence supported the continuous monitoring of the implementation that resulted in an escalation through the use of a plan of action and milestones (PO&AM) document. The PO&AM was a risk management plan, reviewed and approved by a higher authority, therefore, the planned implementation of security controls and the measure of its success was approved at a *different level* of authority from that of Subject. (Section III, Tab D, 13A, pg. 1) After several attempts, the PEX server was eventually taken offline and rebuilt to implement the security controls, similarly demonstrating that while mitigation efforts initially failed, countermeasures were taken. (Section III, Tab C (4), pg. 29, lines 17-21) Also, the ECO/ Vulnerability Manager attested to the fact that the Officer in Charge was a signatory on the PO&AM submitted higher

testifying that, “*it was signed by our OIC.*” (Section III, Tab C (4), pg. 30, ln. 11) The PO&AM was signed by the Previous Flight Commander. (Section III, Tab D, 13B, pg. 2)

Based on the ECO witness testimony, there was very little impact to the users of the system due to a web-based option resulting in minimal loss of “text” service. (Section III, Tab C (4), pg. 29, 20-21) When the IO asked Complainant if Subject’s actions or lack thereof, actually affected the mission, Complainant responded negatively and stated, “*I don’t know that I would say, um, that anything he did while I was there, um, had an immediate impact on the mission one way or the other.*” (Section III, Tab C (1), pg. 71, lines 8-14)

CONCLUSION/FINDING.

Based on the preponderance of evidence, the IO concluded that there was no violation of rule, law, or regulation. None of the witnesses interviewed provided evidence to support Complainant’s allegation that Subject failed to implement security controls on the PEX server. On the contrary, the continuous monitoring of the implementation resulted in an escalation through the use of a PO&AM document. Subsequently, the patches were implemented through a complete system rebuild. Each witness interviewed provided support of a Cyber Security program that involved several echelons of engagement, specifically designed to mitigate “high risk” vulnerabilities. Despite Complainant’s assertion that Subject had negatively influenced the remediation of the vulnerability, anecdotal evidence non-specific to the PEX vulnerability weighted against the other factors, did not meet the standard of preponderance. IAW AFI 17-101, Subject conducted a functional mission analysis given the role of the system in the unit, security protocols, impact, staff, and the unit’s priority of effort at the time. There is no evidence that a violation of a rule, law or regulation occurred given the shift in priorities based on the mission.

Based on the preponderance of evidence, the allegation that between 27 January 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, failed to implement countermeasures to the Patriot Excalibur (PEX) servers, to mitigate “critical or high risk” vulnerabilities identified as Tier I in violation of AFI 17-130 *Cybersecurity Program Management* Allegation 1 is **NOT SUBSTANTIATED**.

ALLEGATION 2. Between 1 February 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, failed to **implement a backup system** of Classified and Unclassified (RADIUS) systems **increasing the probability of “catastrophic” data loss impacting National Security Systems** in violation of AFI 17-130, *Cybersecurity Program Management*.

STANDARDS.

AFI 17-130 *Cybersecurity Program Management*, 13 Feb 20.

3.2. Identify. Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. This function will:

This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside Inspector General channels without prior approval of the Inspector General (DAF/IG) or designee

CUI

3.2.3. Perform a cybersecurity Functional Mission Analysis to identify how IT are interconnected and what the mission impacts are in the event of degradation or outages. The analysis will include understanding how the IT interacts, affects, and is affected by other IT and countermeasures passively and actively operating with the IT. (Section III, Tab D (7A), pg. 8)

REVIEW OF FACTS, PERTINENT TESTIMONY AND DOCUMENTATION

- Complainant discussed the potential for exploitation of vulnerabilities and concluded, *“Um, you know, I -- I could say that there were a lot of things that were degraded because of his [Subject] directions, um, that shouldn’t have been degraded and that had he not issued directives not to do certain things, those things would have been restored to, um, fully operational status.”* (Section III, Tab C (1), pg. 71, lines 22-25)
- Complainant testified that, *“A minor failure would not result in a mission critical issue, where again, using the simple example of the RADIUS server.”* (Section III, Tab C (1), pg. 72, lines 1-2)
- According to Complainant in an email addressed to Subject concerning the priority of tasks submitted by Complainant, *“Like nearly every piece of major equipment in SCOO, the RADIUS (All of them) are single points of failure without any redundancy or any plan of action (with supportive hardware) in place to provide even the basis for common redundancy.”* (Section III, Tab D(1.D), pg. 3(c))
- Complainant continued in the email to Subject, *“This along with system outages in general, have become the accepted standard in SCOO to the point where even the most simple, basic and inherent capabilities for equipment redundancies are completely ignored.”* (Section III, Tab D (1.D), pg. 3(c))
- Complainant also stated, *“To wit, when the RADIUS server in item ‘b’ above [reference to a previous RADIUS failure] was restored, only a single hard drive was used even though the server hardware intrinsically supports RAID levels allowing for redundancy of several types.”* (Section III, Tab D (1.D), pg. 3(c))
- According to Complainant in an email addressed to Subject, *“Our position at recovery was that a readily available second drive would be installed the following weekend to eliminate the single point of failure represented by the sole boot drive. Time and opportunities passed but there was no interest in installing the second drive despite my repeatedly voicing my concerns on a weekly basis over the potential failure of the single drive and widely acknowledged fact that no one in EADS was currently capable of rebuilding the server.”* (Section III, Tab D (1.D), pgs. 3-4(c))
- Subject replied to an email to Complainant regarding RADIUS and other issues, *“The issues you identify below the technical challenges, complacency, training amongst others ring true to me.”* (Section III, Tab D (1.D), pg. 1)
- Subject continued and stated, *“I probably don’t really understand all of the issues you and your teammates face, are you truly the lone voice advocating for change to happen quickly?”* (Section III, Tab D (1.D), pg. 1)
- When the IO asked the Assistant Section Chief about the criticality of the RADIUS he testified that, *“Uh, Radius is, uh, the Radius is a fun one. Uh, for years, we did without a*

Radius, um, this goes back to STIGs, the Security and Technical Implementation Guide, DISA kicks those STIGS out or NSA, through DISA, kicks out a STIG, and basically, uh, let's just say 450 changes have to occur on a Windows 10 box. Um, Adobe has to be, um, 56 security settings have to be done, um, multi-function printers, a STIG would tell me that 26 items have to be done. so, switches, core switches, they all, everything has a Security Technical Implementation Guide, and it's up to us to do these assessments and to change and to make sure that all our systems are locked down. Fortunately, the Air Force does a bit of this work for us, but Radius, if you don't build a server that handles switch authentication, some of the remediations are that you actually have your infrastructure folks go into the switch and they lock the switch down based on one computer to one port based on the network address, or the MAC address.” (Section III, Tab C (3), pg. 46, lines 4-17)

- The Assistant Section Chief further detailed the criticality of the RADIUS and attested, *“Radius was never a requirement. Radius makes life easier, but if you had a sticky MAC, then you could do without a Radius Server.”* (Section III, Tab C (3), pg. 46, lines 19-20)
- When the IO asked the IT Specialist, SCXP he testified, *“I know RADIUS servers are used for, uh, authenticating, um, workstations to the network, and that, uh, um, not too long ago, our folks, I think had set --they had set one up, uh, in order for users to be able to take their workstation in a port jack in the wall and pick it up and move it to another port jack in another room, without having to call the help desk, um, and make them do a manual change on the switches.”* (Section III, Tab C (6), pg. 10, lines 6-10)
- When the IO asked about conversations about critical vulnerabilities, the IT Specialist, SCXP answered, *“But I don't recall anything where it was yes, this is going to fail tomorrow; this is critical; we need to get this fixed.”* (Section III, Tab C (6), pg. 43, lines 7-9)
- The IO asked if the RADIUS server was commercial off the shelf (COTS) and the witness answered in the affirmative and stated, *“We also rely on -a lot on commercial off-the-shelf manuals.”* (Section III, Tab C (7), pg. 11, lines 18-22)
- When the IO asked Subject about the top 5 priorities or projects, Subject attested to the fact that, *“Things failing, I mean there were numerous is what I'm getting at and um, any of that really stick out in mind. I mean the biggest ones we were working on was we were implementing the NORAD NORTHCOM different network; that was a huge undertaking because we were replacing our Air National Guard SIPR network with the NOSC.”* (Section III, Tab C (8), pg. 7, lines 16-20)
- When asked about Subject's priorities at the time, the Section Chief stated, *“So really, our overall mission would be, you know, supporting ADS -- the 224th ADS -- making sure they have full capabilities to do their job, as well as our priority during that time when he came into the flight was to implement that NORAD NORTHCOM SIPR, so that was really our priority was to focus on that, to make sure operations could do their job.”* (Section III, Tab C (5), pg. 34, lines 10-14)
- Subject stated that during the time period in question he was, *“Consumed by primarily personnel issues.”* (Section III, Tab C (8), pg. 8, lines 13-14)
- When the IO asked about mission effectiveness, the Section Chief also noted personnel issues, *“We had a lot of struggles. Personally, there was a lot of changeover in that office, so everyone was learning.”* (Section III, Tab C (5), pg. 9, lines 22-23)
- When questioned by the IO whether there would be data loss in the event of an outage of the RADIUS server, Subject testified, *“Um, but there would be no data loss. In the allegation it says catastrophic data loss. There's no data loss. Basically within -- if there's a problem with the Radius Server and then that translates to problems in the network, systems can't talk*

to each other, but they still contain all their data.” (Section III, Tab C (8), pg. 27, lines 23-25)

- When the IO asked Subject to explain the Western Air Defense role in relation to the Eastern Air Defense role he testified, “*So, if our mission, if we’re unable to execute the mission for whatever reason, WADS will take responsibility of the entire air picture for the continental United States and vice versa. But, these systems do not impact the mission system, so even if our NIPR goes down, that’s a business now, our mission system is still up and running, we don’t fail necessarily. There are services that have received over the NIPR Net, but we have work arounds for that, um, to get them those without NIPR Net being available. So, just because the Radius Server goes down, that certainly does not mean that our mission fails.*” (Section III, Tab C (8), pg. 28, lines 10-14)

ANALYSIS.

Based on the NIST definition, *National Security Systems* excludes a system that is to be used for routine administrative and business applications. Subject and several witnesses denied the use of the RADIUS server as a mission system; the RADIUS servers contain a protocol that allows users to authenticate to the network, controlling access to business systems. For users, the RADIUS servers enabled the ability to move desktops and laptops without configuring the system information at the switch. In recognizing the importance of the service the RADIUS servers provide, multiple witnesses identified a “work around” in the event that there was a loss of service. (Section III, Tab C (8), pg. 20, lines 20-22) A few witnesses characterized the RADIUS servers as essential but not critical to the weapon systems and operational missions.

Witness testimony and evidence indicated, that an outage would not be *catastrophic* because it would not restrict network access, merely the ability to move laptops or desktops around the office. The work-around involved a service request that required the coordination of two sections within the unit, support and infrastructure. Subject noted that a disagreement regarding the roles and responsibilities of RADIUS server maintenance created the need to clearly define each section’s responsibilities of support. Other witnesses testified that the “conflict” resulting from personnel issues was time consuming, such that it detracted from cooperation required to complete RADIUS server maintenance. (Section III, Tab C (8), pg. 23, lines 8-10) The need to remediate the RADIUS server was a day-to-day maintenance routine operation rather than a real risk of degradation that would significantly impact operations. A witness from the Plans and Program office supported that statement and indicated he “*didn’t recall*” a critical need to upgrade the system. (Section III, Tab C (6), pg. 43, lines 6-9) Complainant perceived Subject’s priorities as misaligned to his own. In a Complainant-provided email, Complainant stated there was a plan in place but that, “*time and opportunity passed.*” (Section III, Tab D (1.D), pgs. 3-4(c)) Subject testified that the major priority at the time was SIPR and that it was, “*difficult to work through with limited resources.*” (Section III, Tab C (8), pg. 11, ln 3) Complainant also stated in an email that he probably did not have the support of the Technicians regarding his recommendations and stated, “*I recognize that my SMEs would vehemently disagree with my prognosis-they do so with most I arrive at despite not offering an explanation or support for said opposition.*” (Section III, Tab D (1.D), pg. 6)

While Complainant viewed Subject's priorities as skewed, AFI 17-130.1.3. *Cybersecurity Program Management* provides "a way to balance" for "Authorizing Officials (AOs), Information System Owners, Program Managers, Information System Security Managers, mission owners, and authorized users" to conduct continual risk analysis weighted against the priorities of the mission and the given resources. (Section III, Tab D (6A), pg. 4) Subject conducted a functional mission analysis given the role of the system in the unit, security protocols, impact, staff, and the unit's priority of effort at the time and properly decided on what the unit priorities are and allocated resources accordingly. Although his decision and priorities may not align with Complainant's, there is no evidence that a violation of a rule, law or regulation occurred given the shift in priorities based on the mission.

CONCLUSION/FINDING.

Based on the preponderance of evidence, the IO concluded that there was no violation of rule, law, or regulation. The RADIUS servers provided defense to the network with the additional authentication capability but did not actually store any data, therefore, there could be no catastrophic data loss. Further, the RADIUS servers were a layer of defense to the business systems on the network. Subject was not in a technical role to advise on the implementation of a backup system as a Supervisor. However, as the Flight Commander, Subject could set the priorities. Complainant alleged that Subject's prioritization degraded capabilities. The priority for the 224 SS was the implementation of a long-term project upgrade to the secure network. An outage of the RADIUS servers, as testified by multiple witnesses, would have minimal impact. The IO found no evidence to demonstrate that a rule, law, regulation or policy had been violated.

Based on the preponderance of evidence, the allegation that Between 1 February 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, failed to implement a backup system of Classified and Unclassified (RADIUS) systems increasing the probability of "catastrophic" data loss impacting National Security Systems in violation of AFI 17-130, *Cybersecurity Program Management* Allegation 2 is **NOT SUBSTANTIATED**.

ALLEGATION 3. Between 27 January 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, failed to track secured hard drives containing classified information in violation of AFI 17-1203, *Information Technology Asset Management*.

STANDARDS.

AFI 17-1203 *Information Technology (IT) Asset Management (ITAM)*, 18 May 2018.

2.7.1.1. Purpose. The purpose of an inventory is to ensure all assets reported on the general ledger and the financial statement exist and can be readily located. Any assets in the possession of the Air Force must be accounted for in DPAS in accordance with applicable

property and financial management policies and as prescribed in DODI 5000.76. (Section III, Tab D (8A), pg. 17)

2.7.2.1. The APO shall initiate an investigation into certain lost, damaged, or stolen property that meets the requirement prescribed in DOD FMR 7000.14-R, Vol 12, Chap 7, Financial Liability for Government Property Lost, Damaged, Destroyed, or Stolen. (Section III, Tab D (8A), pg. 18)

2.10.4.2. All media being disposed of or transferred to DLADS or another entity outside of the DOD will be sanitized and/or destroyed as applicable according to AFMAN 17-1301. (Section III, Tab D (8A), pg. 21)

A2.2.3. Property Administrator (PA).

A2.2.3.4. Processes receipt, transfer, and disposition of all IT assets in DPAS. ((Section III, Tab D (8A), pg. 55)

Table A2.1. Crosswalk of roles in DPAS and roles prescribed in paragraph 1.2. (Section III, Tab D (8A), pg. 54)

REVIEW OF FACTS, PERTINENT TESTIMONY AND DOCUMENTATION

- The ECO provided a memorandum for record as proof of the moratorium on asset inventories. The document states, “The requirement to perform an annual physical inventory of IT assets IAW AFMAN 17-1203, paragraph 2.5.5 is temporarily waived.” (Section III, Tab D (5A))
- The ECO provided a CY2020 hand-receipt for the SCOO. Subject was not the hand-receipt holder. (Section III, Tab D (5B), pgs. 1-70)
- The ECO provided a current hand-receipt dated 1 January 2022. Subject was not the Hand receipt holder. (Section III, Tab D (5C), pgs. 1-67)
- When the IO asked about E-waste, the Assistant Section Chief testified, “*Sure, sure. E-waste process for us, I believe, was a facilities program kicked out by the Air Force that basically cleans up electronic waste. Our facilities, uh, our logistics, individuals have dropped a bin, that’s how we use it, they dropped a bin off at our Classified Building in the back out next to the smoke pit, and any cables, any electronic, uh, equipment, keyboard, you’re not supposed to throw it in the garbage, it’s supposed to go into the bin, and all Work Centers for the entire facility will take their electronic waste equipment, stuff that’s not tracked via ADPE, drop in the E-waste bin. When it’s full, uh, we notify our Logistics Work Center, and you know, call whatever company that they have on file for E-waste, and they’ll schedule a truck to show up and take [it].*” (Section III, Tab C (3), pg. 26, lines 16-25)
- The Assistant Section Chief further attested to the frequency of E-waste collection, “*E-waste, and that’s about a month by month basis, uh, if the bin gets full, then somebody has*

to come get it, just kind of like the garbage truck. Comes every week.” (Section III, Tab C (3), pg. 28, lines 19-25)

- When asked by the IO about the classified equipment turn-in process, the ECO testified, *“Classified equipment we take the -- remove the hard drive, and degauss the hard drive, and remove all the markings from the computer, and from the hard drive. Then we have a spreadsheet of the hard drive that -- that had been degaussed with the exception -- currently now there are -- if any new system that comes has solid state drives. So, the solid state drives can't be degaussed. We have to actually -- we have to destroy them. So, we have to go down to the AFRL to destroy the solid state drive. But currently for the equipment that is set for DRMO now, they don't -- they're older pieces of equipment, so they don't solid state drives. So, we degauss the hard drive, and remove it from that system, from the chassis, and, so, the chassis gets DRMO'd, the chassis gets put in a box. We don't put the hard drive back in the -- in the computer.”* (Section III, Tab C (4), pg. 22, 15-25)
- The ECO stated, *“That is I track all of the IT equipment in the unit as far as acquisitions up until the time that the com -- systems are transferred to DRMS. So, I use- it's called DPAS database to record all of the equipment when it comes in, any equipment that's transferred either within, or outside of the unit. And I generate the forms to prepare the equipment for disposition.”* (Section III, Tab C (4), pg. 5, lines 1-4)
- When the IO asked about something that couldn't be concentrated on due to mission, the ECO stated, *“And the -- the ADP, or the -- the -- as the ECO, I wasn't able to -- well, at the time there was a moratorium on inventories, so we couldn't do any inventories because of COVID. So, we kind of had to rely on -- they call it FORGE, it's a byte that the Air Force uses. It has all of your -- your infor -- like computer and server information.”* (Section III, Tab C (4), pg. 11, lines 19-22)
- The Section Chief testified that, *“We get this notification from Logistics. Lets us know that, hey, Rome labs is not taking DRMO at this time or Syracuse is not taking DRMO at this time.”* (Section III, Tab C (5), pg. 21, lines 9-14)
- When the IO attempted to clarify the DRMO process, the Section Chief testified, *“If it's a hard drive specifically, you will -- you will -- you will degauss it, take the stickers off of it. You will sticker it. I can't remember the name of the sticker. [ECO] would be able to tell you that. [The ECO] prints them all off for everybody. You sticker it. The sticker has the serial number on it of the system it came out of and you are signing that sticker saying, this hard drive has been degaussed. And then from that point on they can be e-wasted. They -- those aren't required to go DRMO.”* (Section III, Tab C (5), pgs. 21-22, lines 21-25; 1)
- The Section Chief further detailed the difference between hard drives and solid state drive disposal and stated, *“If it's a different -- a solid state drive, those have to be shredded or pulverized in a different type of -- they can't be degaussed and go through our degausser; have to be shredded or pulverized. Those too, once they're pulverized, would not go to DRMO.”* (Section III, Tab C (5), pg. 22, lines 3-6)
- When the IO asked the Flight Chief if he ever heard the Subject say to trash a classified drive he stated, *“Negative, never, ever. We do have strict procedures that we do for disposition of classified systems, and every time that that has come up, we have followed those procedures to the letter. Never, ever have I heard [Subject] even suggest anything like that.”* (Section III, Tab C (7), pg. 14, lines 14-16)
- When the IO asked whether any of the witnesses had heard of a secure hard drive being disposed of improperly or heard of the suggestion of improper disposal, all five of the

witnesses questioned denied knowledge. The Previous Flight Commander, who had was no longer directly managing the squadron at the time, was not questioned about the allegation. The alleged violation put forward by the complainant is an action or decision made by subject in this case.

- Subject testified when asked about the disposal of classified hard drives, *“If I had been aware of that, it would have been an issue I would have taken action on, so I do know the significance of that and there is very, I guess close or scrutiny in tracking on that from higher authority, I believe I would have been informed if there was any issues with that, but I have no knowledge of any problems with destruction of classified hard drives.”* (Section III, Tab C (8), pg. 29, lines 1-5)
- Subject further testified, *‘that they must go through and it includes degaussing the hard drive, which is just a magnet they use to scramble the data, and um, I believe they have to report it and then I think they have to actually crush it with a hammer and um, and that’s the process they have to go through. So, if there was a problem if there was an issue, I wouldn’t know what to do, I’d have to ask whatever higher authority was, you know, that is responsible for overseeing that process, what the appropriate action would be.’* (Section III, Tab C (8), pg. 30, lines 8-14)

ANALYSIS.

Each witness interviewed regarding the allegation of improper disposal of classified hard drives indicated the process of disposal in detail. There are two methods of equipment disposal used within the 224 SS. The first method of disposal is the E-waste program managed through a commercial logistics contract. A collection point is centrally located behind the buildings for the disposal of items not tracked through the ADPE process (i.e. keyboards, mouse, monitors, and cables). Any unit member may dispose of these types of items in the available bins. Once the bins are full, the items are collected by the contracted company and taken off-site for disposal. The second method of disposal involves items that are classified and tracked through ADPE. These items that were labeled, are tracked in a database of asset inventory called DPAS and disposed of through a process handled by the ECO, whose primary duties are within SCOO. Several witnesses attested to the sanitization process prescribed for the disposal of classified hard drives. The solid state hard drives must be removed from their chasses, then pulverized at AFRL; they are not returned to DRMO. (Section III, Tab C (4), pg. 22, 15-25) Other hard drives are sanitized, stickered, inventoried, and discarded.

IAW AFI 17-1203, an individual must be assigned a role in DPAS to make modifications. The ECO was assigned that role. Subject was not the hand receipt holder. Rather, the SCOO inventory was assigned to a Technician, therefore, Subject did not have direct access to the accountability database or the authority to add, update, or delete the inventory. Further, a moratorium on the inventory of assets prevented the regularly scheduled DRMO turn-in procedures or physical inventory. Given the moratorium, it is more likely than not the SCOO work center was authorized to store classified materials, and contained assets awaiting sanitization and disposal. A loss of an ADPE asset would have resulted in a Report of Survey IAW 17-1203. No additional details regarding the incident were garnered from witnesses. The only witness suggested by Complainant has since separated from the Air

Force and was unavailable for comment. Lastly, Subject denied directing anyone to “trash” a classified hard drive. (Section III, Tab C (8), pg. 30, ln. 25).

CONCLUSION/FINDING.

The ECO and other witnesses detailed the process prescribed in AFI 17-1203 for the handling of classified materials. Each witness indicated that the unit took the handling of classified materials seriously and indicated that, if alerted, would seek assistance from a higher authority, as mishandling of classified materials is a security incident. Further, the inventory requirement of a serialized ADPE item would have resulted in an investigation, once the loss was discovered. Subject and all other witnesses in the leadership chain denied knowledge of an incident or the loss of a secure hard drive. The only witness, other than Subject, was separated from the Air Force and could not be contacted for questioning. No evidence was presented to support the allegation that Subject directed the improper disposal of hard drives, therefore, the IO found that no policy, rule, law, or regulation was violated.

Based on the preponderance of evidence, the allegation that between 27 January 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, failed to track secured hard drives containing classified information in violation of AFI 17-1203, *Information Technology Asset Management* Allegation 3 is **NOT SUBSTANTIATED**.

ALLEGATION 4. Between on or about 1 February 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, directed the improper disposal of classified IT hardware, in violation of AFMAN 17-1301, *Computer Security (COMPUSEC)*.

STANDARDS.

AIR FORCE MANUAL 17-1301 COMPUTER SECURITY (COMPUSEC), 12 Feb 2020.

5.1.3. Risk Management. Utilizing remanence security within an organization is a risk management process that involves the information owner, Information System Owner, Information System Security Manager, Information System Security Officer, Wing Information Protection, and security assistant/manager to make a determination of potential impact prior to sanitizing media or devices for reuse or disposal. The decision is based on a complete risk analysis that involves the identification of organizational mission, mission impacts, threats, and possible compromise to the information system or information. A thorough cost benefit analysis coupled with mission priorities provides the framework for this decision. (Section III, Tab D (9A), pg. 33)

5.2.2. Sanitization of classified devices follows the National Security Agency/Central Security Service Policy Manual 9-12, *NSA/CSS Storage Device Sanitization Manual*, and involves the

This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside Inspector General channels without prior approval of the Inspector General (DAF/IG) or designee

CUI

destruction of the media and/or data via degaussing, incineration, disintegration, shredding, embossing/knurling, chopping/pulverizing/wet pulping (paper), grinding, strip shredding/cutting, or power removal (dynamic random-access memory, static random-access memory, and volatile field programmable gate array). The sanitization/degaussing/destruction of classified solid state and/or magnetic media requires a witness/validator. (Section III, Tab D (9A), pg. 34)

5.2.2.1. Degauss (hard disk drives/diskettes) – Process for reducing the magnetization of a storage device to zero by applying a reverse (coercive) magnetizing force, rendering any previously stored data unreadable and unintelligible, and ensuring that it cannot be recovered by any technology known to exist. Classified information technology storage media cannot be declassified by overwriting per DoDM 5200.01, Volume 3. (Section III, Tab D (9A), pg. 34)

AFI 17-1203 *Information Technology (IT) Asset Management (ITAM)*, 18 May 2018.

2.3.6. Equipment Control Officer (ECO).

2.3.6.2. Will process the receipt, transfer and disposal of all IT assets and complete necessary documentation to establish custodial responsibility. (Section III, Tab D (9B), pg. 9)

2.4.2.2. Controlled Inventory assets must be accounted for in DPAS in accordance with Attachment 2 due to their capability to process and/or transmit personally identifiable information or another sensitive agency information according to DODI 5000.64. (T-0). Physical accountability of these items is required in support of IT configuration management and cybersecurity requirements. Physical accountability supports the goal of automating the association of IT assets with network configuration management items and to enhance overall cyberspace situational awareness of physical assets. . (Section III, Tab D (9B), pg. 12)

2.10.3.1. The asset must have met all IT hardware sanitization requirements in accordance with AFMAN 17-130 and NSA/CSS Policy Manual 9-12. (Section III, Tab D (9B), pg. 21)

REVIEW OF FACTS, PERTINENT TESTIMONY AND DOCUMENTATION

- The ECO provided a memorandum for record as proof of the moratorium on asset inventories. The document states, “*The requirement to perform an annual physical inventory of IT assets IAW AFMAN 17-1203, paragraph 2.5.5 is temporarily waived.*” (Section III, Tab D (5A))
- The ECO provided a CY2020 hand-receipt for the SCOO. Subject was not the hand-receipt holder. (Section III, Tab D (5B), pgs. 1-70)
- The Section Chief testified that, “*We get this notification from Logistics. Let’s us know that, hey, Rome labs is not taking DRMO at this time or Syracuse is not taking DRMO at this time.*” (Section III, Tab C (5), pg. 21, lines 9-14)

This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside Inspector General channels without prior approval of the Inspector General (DAF/IG) or designee

CUI

- The Section Chief testified, *“As far as for ADPE for DRMO equipment, that would be [ECO]. [ECO is] the equipment custodian. She would be able to supply documentation of any equipment that went to the DRMO process. I can tell you that the DRMO has been suspended because of COVID, so a lot of this equipment is still physically in the e-compound awaiting to be disposed of.”* (Section III, Tab C (5), pg. 20, lines 20-24)
- The IO asked that in the event of the disposal of a classified piece of IT equipment, what the procedure would be and the Flight Chief testified that, *“So, if we had, for example, a laptop that was classified, we would remove the hard drive from that, which would be the classified storage. We have a degausser, which is certified for destruction of classified hard drives. We would degauss the hard drive, and then it would go to our DRMO manager, and all the paperwork would be filled out, tagged, and then sent to DRMO after it had been degaussed and declassified.”* (Section III, Tab C (7), pgs. 14-15, lines 23-25; 1)
- When the IO asked the Flight Chief if he had ever seen laptops and desktops in the dumpster behind the building he replied, *“No, computer equipment like that does not go into the dumpster at all, it goes into our DRMO bin and storage area in our -- in our SCOO Work Center.”* (Section III, Tab C (7), pg. 16, lines 8-12)
- The Flight Chief testified that, in the event classified IT equipment was improperly disposed of, he would, *“call the security manager of the site to report the incident.”* (Section III, Tab C (7), pg. 14, lines 1-2)
- After Subject denied knowledge of any improper disposal of classified IT hardware, he noted that he would have to check with the ECO and stated that, *“No, I’ve never directed the disposal of IT equipment at all. It’s a day-to-day function of that work center. It’s nothing that I was directly involved in.”* (Section III, Tab C (8), pgs. 34-35, ln. 25; 1)

ANALYSIS.

Several witnesses attested to the process of disposal of classified IT hardware to include the sanitization procedures. IAW AFMAN 17-1301, classified IT hardware with a solid state drive would have the hard drive removed from the chassis and the media pulverized in the Rome Labs facility. (Section III, Tab C (5), pg. 18, lines 10-24) Once the hard drive was removed and pulverized, it was discarded. Other items such as peripherals or serialized equipment not tracked in ADPE are discarded in the E-waste bin (i.e. mouse, monitor, and keyboard). Lastly, hard drives that are not solid-state drives, are removed, demagnetized/degaussed to scramble the data and disposed of through the DRMO process. IAW AFI 17-1203 the disposal process includes paperwork to track the serialized items, marking the drives, and creating a transaction in DPAS to send the items to DRMO. (Section III, Tab C (7), pg. 16, lines 8-12) At least four witnesses explained the disposal process in-depth and noted that the unit took classified equipment seriously. Witnesses who were interviewed from the chain of command were unaware of any reported incident regarding improper disposal of classified IT equipment. One witness attested, that if made aware of the violation, he would notify the on-site Security Manager. (Section III, Tab C (7), pg. 14, lines 1-2) According to the ECO, *“DRMO people would -- they would call, or send an email,”* if an occurrence happened. (Section III, Tab C (4), pg. 19, ln. 10)

A moratorium of assets prevented the turn-in and physical inventory of equipment from 9 May 20 until after 31 Mar 21. There were no witnesses who could attest to having heard Subject direct the improper disposal of classified IT equipment concerning. Subject

was not a SCOO hand receipt holder and had no knowledge of “disposal issues.” (Section III, Tab C (8), pg. 29, lines 4-5) The disposal of E-waste is the responsibility of the Logistics section of the unit and executed through a contract. Additionally, the DRMO responsible management official is the ECO. Although Subject had oversight authority over the SCOO, Subject was not responsible for the disposal of classified IT equipment and did not have the authority to direct the DRMO prescribed disposal process IAW AFI 17-1203. Lastly, Subject, whom the IO determined was credible, testified that he did not direct the improper disposal of classified IT hardware. (Section III, Tab C (8), pgs. 34-35, ln. 25; 1)

CONCLUSION/FINDING.

Complainant provided anecdotal evidence that was not supported by witness statements or surrounding facts. A moratorium during the period in question was in place. Based on the preponderance of evidence, the IO concluded that pulverizing solid state drives at AFRL was temporarily suspended for accountable secure drives. There was no evidence of loss as a result of the modified procedures. The directives that govern the proper disposal of serialized classified IT equipment prescribes a process that requires the cooperation of the hand-receipt holder, the individual disposing of the equipment, and the ECO. There is no substantive link between Subject and the improper disposal of classified IT equipment. Based on the preponderance of evidence, Subject violated no rule, law, or regulation.

Based on the preponderance of evidence, the allegation that between on or about 1 February 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, directed the improper disposal of classified IT hardware, in violation of AFMAN 17-1301, *Computer Security (COMPUSEC)* is **NOT SUBSTANTIATED**.

ALLEGATION 5. Between on or about 27 January 2021 and 5 Feb 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, directed the destruction of government property, to wit: usable, unclassified desktops and laptops still under warranty, in violation of AFI 17-1203, *Information Technology Asset Management*.

STANDARDS.

AFI 17-1203 *Information Technology (IT) Asset Management (ITAM)*, 18 May 2018.

2.3.6. Equipment Control Officer (ECO).

2.3.6.2. Will process the receipt, transfer and disposal of all IT assets and complete necessary documentation to establish custodial responsibility. (Section III, Tab D (10A), pg. 9)

2.4.2.2. Controlled Inventory assets must be accounted for in DPAS in accordance with Attachment 2 due to their capability to process and/or transmit personally identifiable

information or another sensitive agency information according to DODI 5000.64. (T-0). Physical accountability of these items is required in support of IT configuration management and cybersecurity requirements. Physical accountability supports the goal of automating the association of IT assets with network configuration management items and to enhance overall cyberspace situational awareness of physical assets. (Section III, Tab D (10A), pg. 12)

2.5.2.5. End user devices might be refreshed at recommended refresh schedule based on industry standards outlined in Table 2. (Section III, Tab D (10A), pg. 15)

REVIEW OF FACTS, PERTINENT TESTIMONY AND DOCUMENTATION

- The ECO provided a memorandum for record as proof of the moratorium on asset inventories. The document states, *“The requirement to perform an annual physical inventory of IT assets IAW AFMAN 17-1203, paragraph 2.5.5 is temporarily waived.”* (Section III, Tab D (5A))
- The ECO provided a CY2020 hand-receipt for the SCOO. Subject was not the hand-receipt holder. (Section III, Tab D (5B), pgs. 1-70)
- The ECO provided a current hand-receipt dated 1 January 2022. Subject was not the Hand receipt holder. (Section III, Tab D (5C), pgs. 1-67)
- When asked about the disposal of IT under warranty, the Assistant Section Chief stated, *“Disposal of equipment under warranty, um, well, um, no, no. Your, your DRMO world is a very specific world, you know, when your equipment arrives on site, you know, that’s all tracked, and it used to be AIM and it’s now DPAS and, uh, me being Assistant Base Equipment Custodian, uh, no, uh, you don’t, everything goes out via DRMO, and if it’s under warranty, well, then that’s caught in the process. I mean, we would have to print out, uh, four different pages of paper per asset that leaves the unit.”* (Section III, Tab C (3), pg. 24, lines 17-22)
- The Assistant Section Chief further detailed, *“So, if something was still under warranty, again, we’re printing stuff out in AIM or printing stuff out in the new system DPAS. Um, it would automatically show, hey, this equipment is still under warranty. You can’t get rid of it. You can only transfer it to another unit if they need equipment. Uh, we do have an E-waste. In our E-waste, from time to time, uh, somebody will come up to us and say, hey, I wasn’t sure this was supposed to be an E-waste and it has an ADPE sticker on it, and we wanted to bring it to your awareness.”* (Section III, Tab C (3), pgs. 25-26, lines 17-25; 1-4)
- The Assistant Section Chief also stated, *“Now, we have had equipment and, you know, it’s a training problem, uh, somehow if Airmen get a hold of, I don’t want to say just Airmen, but if people get a hold of some equipment that they’re going to take out to the E-waste for disposal, and an ADPD sticker is found, well, that’s something being tracked in DPAS and it needs to go out the proper channel. If it doesn’t go out, it goes out through the DRMO process, and we’ve had that come up, and it’s good that we’ve had that come up. I mean, people are aware enough to notice the ADPE stickers affixed to systems under warranty.”* (Section III, Tab C (3), pg. 26, lines 6-12)
- When asked about the disposal of IT under warranty, the Section Chief testified that, *“As far as for ADPE for DRMO equipment, that would be [ECO]. [ECO is] the equipment*

custodian. [ECO] would be able to supply documentation of any equipment that went to the DRMO process. I can tell you that the DRMO has been suspended because of COVID, so a lot of this equipment is still physically in the e-compound awaiting to be disposed of.” (Section III, Tab C (5), pg. 20, lines 20-24)

- The IO found that the majority of the assets on the CY2020 hand receipt provided were older than 3-4 years (i.e. CY2016) at the time period in question. (Section III, Tab D (5B), pgs. 1-70)
- The Section Chief testified when asked about the allegation, “*No, IT equipment is not disposed of if it's under warranty. We have a e-waste bin outside of -- as far as -- I'm speaking on behalf of my office. If it's out of warranty and it's not tracked in ADPE, which [ECO] manages, if it is tracked in ADPE, it will go through the DRMO process, which will throw out paperwork, wipe the hard drive, prep the equipment and then we send it off to Rome Labs down the hill and they send it to the program DRMO. If it's e-waste, we have an e-waste bin outside the building. If it's a monitor still under warranty, we'll call those out. If it's a laptop, it's still under warranty, we will call it out to -- depending on the brand. If it's HP, we'll get a technician there. Everything that goes into e-waste is either can't be reused, it's physically broken and can't be repaired or it's out of warranty and we no longer need it. We do -- we do not dispose of equipment under warranty.*” (Section III, Tab C (5), pg. 18, lines 10-24)
- When the IO asked if the ECO ever witnessed the disposal of IT equipment under warranty the witness testified, “*So, if -- so, if by chance equipment was accidentally put in the box to get driven down to Rome Lab, at some point DRMO would say, hey, look, you know, I've looked in DPAS, we can't get rid of this. Is that -- is that how it works? How would that -- how would that process work? The DRMO people would -- they would call, or send an email, and say, you know -- because it has -- there has to be a spreadsheet in the box of all -- everything that's in the box. So, there has to be a spreadsheet along with they call it the 1348-1, which actually are affixed to the equipment.*” (Section III, Tab C (4), pg. 19, lines 1-13)
- The ECO recalled an incident that involved a laptop under warranty that was being turned in, “*There was one -- I do believe there was one laptop that -- because we had [Airman] gathering up equipment for us that needed to be DRMO'd. He did list one laptop that was on his list, and I'm not blaming him because, you know, he's just gathering equipment, so he's not necessarily looking, but then I did see that, and I said, oh, this is still under warranty. And when I told [Complainant], I said, yeah, he's got -- you know, there's a laptop here, but it's still under warranty, I'm not going to DRMO that, and, you know, he -- he kind of got upset, you know, about it, you know, with [Airman], and I don't know, you know. Him and [Airman] were, you know, oil and water, so, I didn't, you know, think too much of it, but I was -- you know, I'm not upset, I said, because, you know, he's just gathering the equipment. It's up to me as the ECO to, you know, look at the -- look at the ex -- the warranty expiration date.*” (Section III, Tab C (4), pg. 20, lines 7-19)
- When the IO asked if the Section Chief ever witnessed the disposal of IT equipment under warranty he testified, “*There's multiple offices that use it for the whole compound, so there's multiple flights, I should say, or offices that will throw equipment out into the e-waste bin, so that could be reported to really anybody. Our LG shop is really the owner of it, of the e-waste program, so they're the ones that make contact with the company to come pick up.*” (Section III, Tab C (5), pg. 19, lines 2-5)
- When asked about the disposal of IT under warranty, the IT Specialist/Plans and Programs

denied having witnessed an incident and stated, *"I have not. And, um, actually, to me, that's one of our, uh, programs here, that we are working on, um, getting up to snuff, regarding life cycle, and so forth -- sustainment. And the -- um, normally, I think most items we get only have a one-year warranty. And, um, that goes in a blink of an eye, so -- So documentation of that would be, you know, um, something that folks would have to reference, if they got it. And most of the stuff that's been here -- you know, we've got stuff that's older. So your best bet, is a lot of stuff is not under warranty anymore."* (Section III, Tab C (6), pg. 21, lines 15-24)

- The IT Specialist/Plans and Programs stated, *"Uh, with my work center, when we get projects in, and so forth, we, um -- we have a spreadsheet where we'll track equipment, and we'll write down serial numbers and things like that, and then date we received it. Um, and that way, we have a method of seeing. And usually, uh, we put in there - 'cause we're not always told what the warranty is. Um, 'cause it could be something that was bought by, uh, Guard Bureau or Air Force, or whoever. And, um, for all we know, it was sitting on the shelf that they had, for a while, and then they give it to us. So we just assume the start date is today and, uh -- when we get it. And then we --we always - one year out is when we go. 'Cause that's typically the way it is. Unless there's some packing slip that says on it that there was a three-year warranty provided and it's been purchased by whoever, uh, that's how you would know. Maybe a packing slip could tell you that there is, uh, a longer warranty than one year."* (Section III, Tab C (6), pg. 22, 3-15)
- After Subject denied knowledge, he noted that he would have to verify the process with the ECO and stated that, *"No, I've never directed the disposal of IT equipment at all. It's a day-to-day function of that work center. It's nothing that I was directly involved in."* (Section III, Tab C (8), pgs. 34-35, ln. 25; 1)
- When the IO asked Subject about IT under warranty, he denied knowledge and testified, *"No. No. When we do the DRMO process, we're actually doing that right now. That gets -- all the DRMO equipment goes through the equipment custodian process; it's very, I guess, detail tracked, there's no really room for error on this, and if there is then it becomes, you know, that's when we have to take the appropriate action, but our equipment custodian has to DRMO all the electronic waste, we do it throughout the entire year, especially go through the process and follow the paperwork to DRMO excess IT equipment and we send that to the, I forget what it's called, but essentially there's a central locations where all electronic waste from the DoD goes, um, you know, and it's an entire DRMO process as part of the equipment custodian program."* (Section III, Tab C (8), pg. 33, lines 12-20)

ANALYSIS.

A moratorium of assets prevented the DRMO turn-in and physical inventory of equipment from 9 May 20 until after 2 Apr 21. The Assistant Section Chief testified that a common training mistake is to attempt to turn-in ADPE tracked equipment through the E-waste bin. The Technician noted that the ADPE stickers indicate to most trained end users that the equipment must go through the DRMO process. Although, the Assistant Section Chief discussed the possibility of improper disposal, he did not recall a specific incident where that had occurred.

The ECO recalled an incident involving a laptop under warranty that was mistakenly collected for turn-in. The ECO attested, *"It's up to me as the ECO to, you know, look at the -- look at the ex -- the warranty expiration date."* (Section III, Tab C (4), pg. 20, lines 18-19) Based on the preponderance of the evidence, a large number of IT assets older than CY2016 in the unit were due for a tech refresh based on AFI 17-1203 Table 2. There were no witnesses who could attest to having heard Subject direct the improper disposal of IT under warranty. Subject, deemed credible by the IO, testified that he did not direct the improper disposal of IT under warranty and testified, *"No, I've never directed the disposal of IT equipment at all."* (Section III, Tab C (8), pgs. 34, ln. 25)

CONCLUSION/FINDING.

A moratorium of asset inventory and the temporary suspension of AFRL pulverization of solid state hard drives occurred during the time period, however, there was no indication that disposal procedures for IT equipment were disrupted. All of the witnesses interviewed were able to provide a detailed description of the turn-in process, indicating that the process was followed by the unit ECO. There were no witnesses to support the allegation that Subject directed the destruction of IT assets (i.e. desktops and laptops) under warranty. Subject credibly testified that he did not direct the destruction of any IT equipment. Based on a preponderance of evidence, the IO determined that no violation of rule, law, or regulation occurred.

Based on the preponderance of evidence, the allegation that between on or about 27 January 2021 and 5 Feb 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, directed the destruction of government property, to wit: usable, unclassified desktops and laptops still under warranty, in violation of AFI 17-1203, *Information Technology Asset Management* is **NOT SUBSTANTIATED**.

ALLEGATION 6. Between 27 January 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, failed to provide communication and information system records (CISR) documentation to Technicians for National Security Systems in violation of AFI 17-101 para. 3.12.3, *Risk Management Framework for Air Force Information Technology*.

STANDARDS.

AFI 17-101, *Risk Management Framework for Air Force Information Technology*, 6 Feb 20.

3.12. Information System Security Manager (ISSM). The ISSM is the primary cybersecurity technical advisor to the AO, PM, and ISO. For base enclaves, the ISSM

manages the installation cybersecurity program, typically as a function of the Wing Cybersecurity Office. That program ISSM may also serve as the system ISSM for the enclave and reports to the CS/CC as the PM for the base enclave. The ISSM:

3.12.3. Ensures all AF IT cybersecurity-related documentation is current and accessible to properly authorized individuals. (14)

REVIEW OF FACTS, PERTINENT TESTIMONY AND DOCUMENTATION

- When the IO asked if there were delays due to COVID considerations the IT Specialist, SCXP answered, *“Yeah, I mean, nobody everybody was teleworking. And, um, only certain people were in here. So there was, um, not much activity, and certainly, not much checking, from my end, on the progress of those.”* (Section III, Tab C (6), pg. 33, lines 3-5)
- When asked about the CISR document, the IT Specialist, SCXP answered, *“Yes, there’s a lot of drawings. So I manage the program from my work center. And we’ve got, I think, four different work centers that they are responsible for different systems. And so I give them training. And, um, they have a particular, um, touch point. The work center will have one person that manages that -- those drawings within their work center.”* (Section III, Tab C (6), pg. 29, lines 7-10)
- The SCXP IT Specialist further detailed, *“Um, I oversee the program, overall, to see if these guys, um, are trained. And once they’re trained, then they manage their own drawings. So each work center will have their own drawings, and they’re told to update them when they have a, um --they’re --by rule or reg, I guess you could say, they’re supposed to inspect them once a year, at the minimum.”* (Section III, Tab C (6), pg. 29, lines 7-15)
- When asked if the chain of command is informed when updates are overdue the IT Specialist, SCXP stated, *“Normally, what I do is, um, I will talk to -- because within the training and in the reg, it says that the work center supervisor is responsible for making sure that the inspections are done on them. And I, as the overseer of the whole program, will check. But, um, I’ve got a lot of duties going on, and so forth. And so it’s usually like -- like I said, every three months or something before I can get multitask clock in -- to get around to that.”* (Section III, Tab C (6), pg. 30, lines 17-21)
- When asked if the issue with updating the CISR document was elevated to the chain of command, the SCXP IT Specialist testified, *“I think the only level it would’ve probably hit is his [Assistant Section Chief], uh, work center supervisor. And, um, the -- you know, it’s kinda like one of those where, um, I don’t control those personnel, and you want it managed inside there. And so you don’t want to like necessarily be, um, confrontational with folks on stuff. But also, it’s, um, not that critical that, you know, you have to start a war over.”* (Section III, Tab C (6), pg. 32, lines 2-6)
- When asked about the frequency of his audits of the document, the IT Specialist, SCXP stated, *“Um, I try to, um, get -- quarterly, I try to look to see where the work centers are at and steer them. Um, several of them have been pretty good at doing that. The SCOO shop, in particular, has been very bad in keeping their up to date. Um, and, uh, so, uh, needs improvement.”* (Section III, Tab C (6), pg. 30, lines 1-4)
- Subject stated that the unit was a geographically separated unit. When asked to clarify, Subject stated, *“So, we’re not on a base, we’re just two buildings shrouded by a fence, um,*

This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside Inspector General channels without prior approval of the Inspector General (DAF/IG) or designee

CUI

and we're, you know, we're a group, we're not a wing." (Section III, Tab C (8), pg. 7, lines 7-8)

- When the IO asked Subject in what capacity he served as the Flight Commander the ISSO or the ISSM the Subject testified that, *"Uh, I wouldn't sign in any of those capacities. That's uh, they're talking about IA, like Information Assurance."* (Section III, Tab C (8), pg. 12, 22-23)
- When the IO asked about the CISR document, Subject testified, *"So, they [Plans and Programs] manage that program and um, and provide it to me and I looked at it before, I've asked them to see them and I've seen them."* (Section III, Tab C (8), pg. 36, lines 6-7)
- Subject further testified, *"You know, there's always a lag, you know, this is -- if you work in IT, this is always a problem in that changes are happening rapidly and it's sometimes the CISR documents fall behind, but to your point, I don't think they are abnormally managed - - we are unusual in any way when it comes to CISR documents. I think they put in the effort to make sure those are accurate, but probably sometimes they're not, just because of normal business. Not maliciously, it's just something that happens, just like a continuous problem in IT, making sure your documentation is up to date."* (Section III, Tab C (8), pg. 36, lines 11-17)
- When the IO asked if Subject viewed the CISR document, he stated, *"Yeah, when I asked for it to see if, um, they sent me the shared drive link, this was a couple of years ago, but I had read-only access to them, which I think makes sense so that they can try to keep the integrity of the document, but you just ask Plans and Programs, you know, they'll tell you where it's at. I'm not sure even if there is any kind of restriction on who can read them."* (Section III, Tab C (8), pg. 35, lines 9-13)

ANALYSIS.

Complainant did not define how Subject, in his role as Flight Commander had violated a rule, law or regulation, therefore, the standards of the RMF for an *Information System Owner* responsible for a base enclave(s) were applied. For base enclaves, the ISSM manages the installation cybersecurity program, typically as a function of the Wing Cybersecurity Office and is responsible for the ensuring all AF IT cybersecurity-related documentation is current and accessible to properly authorized individuals. Subject denied having a role as ISSM of the base enclave and attributed the role to Information Assurance. (Section III, Tab C (8), pg. 12, 22-23) National Security Systems or mission systems, as referenced in the 224 SS, were not maintained by SCO.

According to Complainant's testimony, *"the CISR drawings are important because, basically these are supposed to show the equipment that's in place, what its function is, how it's interconnected to other equipment and, you know, what -- what its function is in the grand scheme of things, as well as who's supposed to maintain it."* (Section III, Tab C (1), pg. 24, lines 11-13) However, Complainant, a newer hire, was unfamiliar with the layout of the server room. Complainant recalled a time when he used outdated drawings for maintenance and was reprimanded by Subject for using "de-commissioned" equipment. (Section III, Tab C (1), pg. 23, ln. 15) Complainant testified that the Assistant Section Chief, responsible for the updates, told him, *"it's never been issued to me as a—as a priority to work on."* (Section III, Tab C (1), pg. 24, ln. 23) The CISR document provides a comprehensive drawing of the network infrastructure. Accurate drawings are used to verify

that Technicians install the correct equipment, in the appropriate location, and are accountable to the correct Information System owner.

The SCXP IT Specialist detailed the CISR document process. The CISR document is comprised of drawings of each work center's area of responsibility. (Section III, Tab C (6), pg. 29, lines 7-15) Each Work Center has a designated point of contact, Work Center Manager, responsible for updating its portion of the drawing. (Section III, Tab C (6), pg. 29, lines 7-10) Updates are sent to the Plans and Programs section iteratively. (Section III, Tab C (6), pg. 35, lines 6-13) The Plans and Programs department then updates the master CISR document. Subject noted that it was available in a "read-only" format on the network. (Section III, Tab C (8), pg. 35, lines 9-13) The SCXP IT Specialist monitors section updates on a quarterly basis with the designated Work Center Managers. The requirement for the inspecting the CISR document is "annually." (Section III, Tab C (6), pg. 29, ln.15) The SCXP IT Specialist testified that the Work Center Manager for SCOO had been routinely, "*very bad*" with updating the sections portion of the CISR document, however, he had not elevated the concern beyond the Section Chief. (Section III, Tab C (6), pg. 30, lines 2-3) In the event of an overdue CISR update from a Work Center Manager, the SCXP IT Specialist testified, "*So that's -- where it ends. Um, the work center supervisor, uh, would be aware of it, in those cases. But that's usually where it ends.*" (Section III, Tab C (6), pg. 31, lines 7-8) He stated, "*Everybody was teleworking,*" as a result of the pandemic which made it difficult to keep everything updated and attested that there was "*not that much activity.*" (Section III, Tab C (6), pg. 33, lines 3-4) The CISR document is designed to understand the base infrastructure support requirements as the communications picture develops. When asked about the CISR document updates, Subject mentioned a "*lag time*" that is not "*abnormal*" compared to other units. (Section III, Tab C (8), pg. 36, lines 11-3) Further, Subject did not have a direct role in the CISR document updates. Based on his role as a Supervisor, if he had been informed by the SCXP IT Specialist that there was difficulty in getting updates from the SCOO section, there may have been updates presented, however, given the priorities of effort and the pending changes to the network, an updated CISR would not be guaranteed.

CONCLUSION/FINDING.

IAW AFI 17-101, the ISSM is ultimately responsible for the provision of an updated CISR to unit personnel, as authorized. When questioned, Subject denied that he served in an ISSM role. (Section III, Tab C (8), pg. 12, 22-23) Subject was not responsible for ensuring that the CISR document was updated. In the 224 SS, the SCXP IT Specialist is responsible for updating the master document, comprised of several overlays, and subsequently, distributing an accurate reflection of the infrastructure. (Section III, Tab C (6), pg. 29, ln. 7) This process relies on each Work Center Manager's integral role in updating their segment of the document, "annually" at a minimum. (Section III, Tab C (6), pg. 33, ln. 22) Evidence was presented that the SCOO Work Center failed to provide the minimally required updates. (Section III, Tab C (6), pg. 30, lines 1-4) However, Subject was not aware of the inaccuracy of this specific work center's CISR drawings, as the responsible management official did not make him aware of the issue. (Section III, Tab C (6), pg. 32, lines 2-6) Further, the Cyber Systems Support work center was not responsible for National Security Systems, as defined. Updating the CISR documentation was not prioritized above other missions. Based on the preponderance of evidence, the Subject did not violate a rule, law, or regulation.

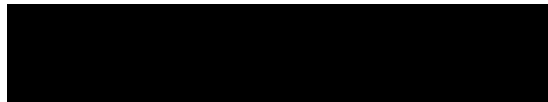
This is a protected document. It will not be released (in whole or in part), reproduced, or given additional dissemination (in whole or in part) outside Inspector General channels without prior approval of the Inspector General (DAF/IG) or designee

CUI

Based on the preponderance of evidence, the allegation that between 27 January 2021 and 31 March 2021, [Subject], 224th Support Squadron, Eastern Air Defense Sector, New York Air National Guard, Rome, New York, failed to provide communication and information system records (CISR) documentation to Technicians for National Security Systems in violation of AFI 17-101 para. 3.12.3, *Risk Management Framework for Air Force Information Technology* Allegation 6 is **NOT SUBSTANTIATED**.



RECOMMENDATION.

We make no recommendations in these matters.



Investigative Operations Specialist, DAF/IG

Section II, Tab D -- Appointing Authority Approval

As directed by the Department of the Air Force Inspector General (DAF/IG), completed this investigation to satisfy the requirements of AFI 51-1102, *Cooperation with the Office of Special Counsel*, in response to an Office of Special Counsel (OSC) tasking (Section III, Tab A). The Investigating Officer found that six of the six allegations against the Subject were not substantiated, therefore, the Tentative Conclusion process was not required. My subsequent review of the ROI found it technically and qualitatively sufficient. Further, I concur with and approve the findings of the investigating officer pending further review and approval in accordance with AFI 51-1102. The original appointing authority for this IG investigation was , Director, Complaints Resolution Directorate (DAF/IGQ).  assumed this position as of 29 Jun 22, and will act as appointing authority for the remaining actions of this case.



Director, Complaints Resolution

REPORT OF INVESTIGATION

OSC FILE No. DI-21-000551

Witness List (Appendix A.)

Section III, C1. **Complainant-** [REDACTED], Former GS-12, Information Technology (IT) Specialist and “IT Lead”, 224th Support Squadron, EADS

Witnesses

Section III, C2. [REDACTED], **Previous Flight Commander**, 224th Support Squadron, EADS

Section III, C3. [REDACTED], **Assistant Section Chief** or Assistant Noncommissioned Officer in Charge (NCOIC) of Cyber Support Operations, Vulnerabilities Manager and Alternate Equipment Control Officer (ECO), 224th Support Squadron, EADS

Section III, C4. [REDACTED], GS-11, IT Specialist and Primary **Equipment Control Officer (ECO)**, 224th Support Squadron, EADS

Section III, C5. [REDACTED], NCOIC or **Section Chief**, Cyber Support Operations, 224th Support Squadron, EADS

Section III, C6. [REDACTED], **IT Specialist, Plans and Programs**, Network Operations, 224th Support Squadron, EADS

Section III, C7. [REDACTED], **Flight Chief**, Cyber Defense Network Operations, 224th Support Squadron, EADS

Section III, C8. **Subject-** [REDACTED], Former Flight Commander, 224th Support Squadron, EADS