



U.S. OFFICE OF SPECIAL COUNSEL

1730 M Street, N.W., Suite 300
Washington, D.C. 20036-4505

The Special Counsel

January 15, 2015

The President
The White House
Washington, D.C. 20510

Re: OSC File No. DI-13-2697

Dear Mr. President:

Pursuant to my duties as Special Counsel, enclosed please find the Department of the Navy's (Navy) investigative report, based on disclosures of wrongdoing at the Naval Undersea Warfare Center Division in Newport, Rhode Island (Division Newport), made to the Office of Special Counsel (OSC). OSC has reviewed the report and in accordance with 5 U.S.C. § 1213(e), provides the following summary of the allegations and our findings.

The whistleblower, Mr. Jeffrey McDuff, a former civilian information technology (IT) specialist at Division Newport, alleged that employees engaged in conduct that constituted a violation of law, rule, or regulation, an abuse of authority, and a substantial and specific danger to public safety by wrongly reporting that high-risk Information Assurance Vulnerability Alerts (IAVAs) were "Fully Compliant" even though they remained vulnerable. Mr. McDuff consented to the release of his name.

The agency investigation did not substantiate Mr. McDuff's disclosures that unmitigated Information Assurance Vulnerabilities (IAVs) posed a risk of manipulation to Division Newport's networks. The agency found no evidence that the information assurance manager (IAM) and the remediation manager (RM) had failed to mitigate known IAVs. Additionally, the agency did not substantiate that the IAM had falsely reported IAVs as being "fully compliant" or had failed to mitigate vulnerabilities. Nevertheless, the agency noted that the investigation highlighted both the confusion that can occur without adequate Information Assurance (IA) training as well as the risk associated with relying on contractors to perform scanning and remediation functions. The investigative report was provided to Division Newport's Commander and to the U.S. Fleet Cyber Command Inspector General for review. In response, Division Newport has taken and plans to take a number of recommended actions, such as providing training to personnel, and updating written policies and procedures to avoid confusion in the future. I have determined that the agency reports contain all of the information required by statute and that the findings appear to be reasonable.

The President
January 15, 2015
Page 2 of 9

On July 3, 2013, OSC referred Mr. McDuff's allegations to Secretary of the Navy Ray Mabus to conduct an investigation pursuant to 5 U.S.C. § 1213(c) and (d).¹ On January 31, 2014, Acting Secretary of the Navy Juan Garcia submitted the agency's report to OSC. The investigation was conducted by the Naval Sea Systems Command (NAVSEA) Inspector General. In response to OSC's request for additional information, the agency submitted a supplemental report on May 2, 2014. Pursuant to 5 U.S.C. § 1213(e)(1), Mr. McDuff submitted comments on the agency's report and supplemental report on June 30, 2014. On November 5, 2014, the agency also provided an update regarding the recommended actions Division Newport has taken and plans to take in response to the agency's report. As required by 5 U.S.C. § 1213(e)(3), I am now transmitting the reports.

I. The Whistleblower's Allegations

Mr. McDuff disclosed that management wrongly reported that high-risk Information Assurance Vulnerability Alerts (IAVAs) were "Fully Compliant" even though they remained vulnerable. Information Assurance Vulnerabilities (IAVs) are issued by the Department of Defense (DOD) to alert commands of the existence of vulnerabilities in their IT equipment.

According to Mr. McDuff, in addition to the Online Compliance Reporting System (OCRS) used by DOD, Division Newport also performs scanning operations of its IT equipment two to three times a day through the Vulnerability Analysis and Remediation System (VARS). VARS is a web portal that was developed internally at Division Newport. The scanning operation examines the IT assets for vulnerabilities that have already been identified by DOD in the issuance of IAVAs.

On April 2, 2013, Mr. McDuff took over the scanning operation of the IT assets. Mr. McDuff disclosed that the scanning operations reported over 2,000 unmitigated IAVs. Of those 2,000 IAVs, 300 were high-risk, posing the greatest threat of external and/or internal cyber-attacks. Moreover, Mr. McDuff stated that he identified approximately eleven high-risk IAVAs that had been reported between 30 and 90 days earlier in OCRS as "Fully Compliant," but were never corrected. Mr. McDuff stated that the IAM is the official responsible for the reporting of the IAVAs as corrected, and the RM is the official responsible for mitigating the vulnerabilities. According to Mr. McDuff, the IAM instructed

¹ The Office of Special Counsel (OSC) is authorized by law to receive disclosures of information from federal employees alleging violations of law, rule, or regulation, gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health and safety. 5 U.S.C. § 1213(a) and (b). OSC does not have the authority to investigate a whistleblower's disclosure; rather, if the Special Counsel determines that there is a substantial likelihood that one of the aforementioned conditions exists, she is required to advise the appropriate agency head of her determination, and the agency head is required to conduct an investigation of the allegations and submit a written report. 5 U.S.C. § 1213(c). Upon receipt, the Special Counsel reviews the agency report to determine whether it contains all of the information required by statute and that the findings of the head of the agency appear to be reasonable. 5 U.S.C. § 1213(e)(2). The Special Counsel will determine that the agency's investigative findings and conclusions appear reasonable if they are credible, consistent, and complete based upon the facts in the disclosure, the agency report, and the comments offered by the whistleblower under 5 U.S.C. § 1213(e)(1).

The President
January 15, 2015
Page 3 of 9

two contract employees to report IAVAs as “Fully Compliant” without correcting the vulnerabilities.

During a meeting between Mr. McDuff and the IAM on April 9, 2013, the IAM admitted that some IAVAs had been reported as “Fully Compliant” even though they were not fixed. The IAM stated that she and the RM agreed to report these IAVAs as “Fully Compliant” because there were plans to correct them within a few days. However, Mr. McDuff stated that the IAM’s justification did not explain why eleven IAVAs had not been fixed as long as 90 days after being reported as “Fully Compliant.”

Mr. McDuff disclosed that the IAM and the RM’s actions were not in compliance with Communications Tasking Orders (CTOs). CTOs are agency-wide directives issued by the Department of the Navy. Specifically, Mr. McDuff identified CTO 11-16, Secure Configuration Compliance Validation Initiative and Vulnerability Remediation Asset Manager (VRAM) Requirements. CTO 11-16 requires that each Command report the total number of vulnerabilities and the total number of corrected vulnerabilities in the OCRS. Additionally, any Command unable to comply with CTO 11-16 is required to submit a mitigation plan.

Mr. McDuff alleged that by directing subordinate employees to report vulnerabilities as fixed, the IAM and the RM were underreporting the total number of known vulnerabilities and misreporting the number of corrected vulnerabilities. Furthermore, they misreported corrected vulnerabilities rather than submitting a mitigation plan outlining how the vulnerabilities would be corrected. By reporting the IAVAs as “Fully Compliant,” the Commander and DOD did not receive email alerts regarding unfixed vulnerabilities. As a result, known vulnerabilities were not being corrected and continued to pose a threat of a cyber-attack. Thus, Mr. McDuff asserted that the two managers’ actions were not in compliance with CTO 11-16. Further, Mr. McDuff alleged that both managers abused their authority by misreporting the number of vulnerabilities while failing to repair them in order to avoid embarrassment.

II. The Agency Report

A. The Investigation

Secretary Mabus tasked the Office of the Naval Inspector General to investigate this matter, who directed the NAVSEA Inspector General to conduct an investigation with collaboration and support from the U.S. Fleet Cyber Command Inspector General. An investigative team comprised of individuals from NAVSEA Inspector General conducted the investigation.

According to the report, the investigative team focused on the detection, remediation, and compliance reporting requirements of IAVs on the Boundary 3 Community of Interest (B3-COI) network at Division Newport between March 27 and April 15. During his interview, Mr. McDuff stated that he was responsible for scanning the B3-COI network from

The President
January 15, 2015
Page 4 of 9

March 27 to April 15, 2013. In addition to Mr. McDuff, the team conducted interviews with three contract employees, the IAM, and the RM. Additionally, the investigative team extracted email files from government computers assigned to Mr. McDuff, the IAM, and the RM.

B. Background Information

In order to facilitate an understanding of the subject matter and the investigation, the report provided background information. The report defined an IAV as a “software vulnerability that an attacker can exploit, potentially gaining unauthorized access to sensitive information.” As a result of this risk, DOD has mandated that all commands scan their IT networks and remediate all vulnerabilities. The report explained that IAVs are divided into three categories based on the amount of risk, from greatest to lowest risk: (1) Information Assurance Vulnerability Alerts (IAVAs), (2) Information Assurance Vulnerability Bulletins (IAVBs), and (3) Information Assurance Technical Advisories (IAVTs). IAVAs are considered the most serious IAVs and pose the greatest risk of exploitation. As a result, commands are required to remediate IAVAs within 21 days of initial notification from DOD.

The report further explained that the Naval Cyber Defense Operations Command (NCDOC) is responsible for reporting incidents and associated analytical results to the U.S. Cyber Command within DOD. NCDOC is responsible for releasing IAV information to Navy commands and provides oversight of commands’ IAV compliance via OCRS. Thus, NCDOC will notify Division Newport that there is a new IAV. Division Newport is then required to acknowledge that it has received the IAV notification in OCRS. Concurrently with the acknowledgment, Division Newport personnel update the eEye Retina scanner, which is the tool used to search the B3-COI network for the IAVs that require remediation by NCDOC. Division Newport also conducts daily scans using eEye Retina to detect IAVs on the B3-COI network. The data is then automatically updated into VARS for viewing. VARS provides a graphic display of the IAVs discovered during the daily scans.

The report stated that Division Newport separates IA and remediation responsibilities between two offices, which are referred to as “Codes.” Code 1153 provides IA functions, including network vulnerability scanning and compliance reporting. The IAM is part of Code 1153. Code 1142 is responsible for remediating identified vulnerabilities by deploying security patches, coordinating with server administrators, and providing security configuration settings. The RM is part of Code 1142.

Lastly, the report noted that prior to Mr. McDuff’s assignment to conduct IAV scans, Division Newport experienced two structural impediments. The first was a contract dispute in January 2013 involving an unsuccessful contract bidder who protested Division Newport’s newly awarded IT Support contract. According to those interviewed, the contract protest directly impacted the IAV scanning and remediation tasks. The second challenge was the lack of a vulnerability manager who would have been responsible for ensuring that IA personnel received daily status updates of vulnerability scans, reporting IAV status in OCRS, and managing disconnection of noncompliant assets.

The President
January 15, 2015
Page 5 of 9

C. Findings

Management Officials' Failure to Mitigate IAVs

The agency investigation did not substantiate Mr. McDuff's claim that the IAM and the RM failed to mitigate IAVs. The investigative team reviewed nine historic scan results of the B3-COI network extracted from emails located on Mr. McDuff, the IAM, and the RM's government computers. The report explained that the investigative team could only review these nine scans because the NCDOC requires Division Newport to retain IAV scan records for a period of 90 days. Since the 90-day-old scan results were discarded within VARS as new scan results were generated, the investigative team relied on these nine scan results because they were the only records available for the relevant time period.

The investigative team reviewed the nine scan results and found that fewer than 300 IAVAs existed on the B3-COI network at any one time. For example, the scan results that Mr. McDuff sent to the RM on April 3 and April 5, 2013, only had 30 and 189 IAVAs respectively. In its review of the scans, the investigative team found that IAVAs varied from as low as thirteen to as high as 253, but it could not find 2,000 unmitigated IAVAs.

The investigative team also interviewed the three contract employees responsible for IAV scanning, remediation, and reporting of the B3-COI network. All three contractors stated that they had never seen 2,000 IAVAs on a daily scan of the B3-COI network. The contractors' statements were confirmed by subject matter experts (SMEs) from NAVSEA Command Information Office who were interviewed during the investigation. The SMEs also stressed the fact that the daily scans are a snapshot of a dynamic network where assets are removed or introduced, and software is installed and uninstalled.

In his comments on the agency report, Mr. McDuff took issue with the investigative team's repeated references to and conclusion that it did not find anywhere close to 2,000 unmitigated IAVAs during its analysis of the nine scans. Mr. McDuff clarified that the term "IAVAs" was used in the broader context throughout his tenure. He noted that there were 2,000 unmitigated "vulnerabilities."

According to Mr. McDuff, the report's reference to the "VARS Scan Results" as indisputable electronic evidence is unequivocally false and points to the investigators' lack of understanding of the technical tools used at Division Newport. Mr. McDuff stated that the eEye Digital Security's Retina Network Security Scanner is the only government authorized vulnerability application used to conduct enterprise-wide vulnerability identification and analysis. The VARS tool, on the other hand, is incapable of conducting any scanning activities. However, the agency report noted that the eEye Retina Scanner is the sole tool used by Division Newport to detect IAVs, and that the data from the daily scans was automatically uploaded into VARS for review and action.

The President
January 15, 2015
Page 6 of 9

The report asserted that Mr. McDuff's training in Division Newport's scanning and remediation process appeared experiential, and he did not have a thorough understanding of IAVs. The report further observed that the lack of a vulnerability manager and the reliance on contractors to conduct scanning functions, coupled with the contract dispute, contributed to Mr. McDuff's misunderstanding of the process. Lastly, the report stated that the reliance on contractors to support IA scanning and remediation programs posed a threat to the execution of IA functions and responsibilities. Although a "hiring freeze" had delayed plans to fill vacant IA positions, the report recommended that conversion of contract positions should be a priority.

The Information Assurance Manager's False Reporting of IAVs in OCRS

The investigation also did not substantiate Mr. McDuff's allegation that the IAM falsely reported IAVs as being "Fully Compliant" in OCRS. Mr. McDuff provided the investigative team with a list identifying fourteen specific IAVAs he believed were incorrectly reported as "Fully Compliant" in OCRS. The investigative team analyzed Mr. McDuff's list by comparing it to the nine historic scan results and to the data reported in OCRS. Additionally, the investigative team interviewed the three contact employees responsible for reporting data in OCRS and reviewed Division Newport's OCRS reporting process.

The investigative team's review of the IAVs identified by Mr. McDuff found that several, but not all, reappeared in subsequent VARS scans even though they had been reported as being "Fully Compliant" in OCRS. However, during interviews, the three contract employees stated that a particular IAV could reappear as an asset's configuration (hardware and software) changed. Further, one contractor stated that she reported IAV compliance based on when a patch was deployed to remediate the IAV, rather than when the patch was successfully installed. All three contractors specified that once a patch was deployed to remediate an IAV, there was still a chance it could be delayed, as in situations in which a server could not be restarted until a later time. The investigative team concluded that the IAVs identified by Mr. McDuff that reappeared following compliance reporting in OCRS were due to asset configuration changes on Division Newport's dynamic network.

In his comments on the report, Mr. McDuff disagreed with the agency's conclusion that the reappearance of overdue IAVAs was attributed to the result of a dynamic network environment. He noted that there were internal policies and procedures to reduce or diminish the effect associated with reappearing vulnerabilities. Specifically, Mr. McDuff pointed to the Change Control Boards (CCB), stating that they are designed to prevent the haphazard practice of installing, updating, or changing a machine's software or configuration in a live environment without first testing those changes before introducing them. Instead, Mr. McDuff opined that previously reported overdue vulnerabilities did not appear on subsequent scans because the device was powered off during the scheduled eEye Retina scan. Mr. McDuff concluded that these vulnerabilities did reappear, however, during unscheduled eEye Retina scans.

The President
January 15, 2015
Page 7 of 9

According to the report, during the interviews the contractors confirmed that even if an unmitigated IAV was reported as “Fully Compliant” in OCRS, it would still show up in subsequent VARS scans. However, the contractors stated that in those situations the asset is manually disconnected from the network after three days in order to reduce the risk of non-compliant IAVs being exploited before they are fixed. Although the agency report did not mention unscheduled scans at Division Newport, it stated that the Naval Network Warfare Command’s CTOs require commands to perform monthly scans. Division Newport’s local Vulnerability Management Plan requires more than the CTO by mandating that scans be performed at least daily. The report also explained that the IAVs identified by Mr. McDuff were not found on subsequent scans, which provided the investigative team with reasonable assurance that personnel were actively addressing them.

Moreover, the report detailed Division Newport’s OCRS reporting process. Division Newport has two internal control mechanisms in place to ensure accurate reporting in OCRS. The first mechanism is the separation of IA responsibilities between Code 1153 and Code 1142. The second mechanism is the separation in systems. More specifically, data in OCRS was manually entered by Code 1153 personnel based on VARS scan results. If Code 1153 personnel entered a misreported remediation action into OCRS, the vulnerability would continue to appear in subsequent scans in VARS and undergo remediation by Code 1142 personnel.

The investigative team found that these internal control mechanisms were adequate to support accurate reporting in OCRS because no single Code executed all the required duties of scanning, remediating, and reporting set out by the NCDOC. The report maintained that Code 1153 and Code 1142 personnel would have to collectively circumvent the internal controls in order to deliberately misreport the mitigation of IAVs in OCRS. This is because if Code 1153 personnel and the IAM falsified compliance reporting in OCRS, the IAVs would still show up on the VARS scan results. Thus, Code 1142 would have to manipulate the VARS scan results to indicate that a remediation action had taken place so that the IAVs would no longer appear. The investigative team’s examination found no evidence of collusion between the two Code’s personnel to misreport IAVs in OCRS. Further, the three contract employees stated that they never falsely reported IAV compliance nor were they ever instructed to do so.

The report also noted that the requirements were unclear for amending a “Fully Compliant” OCRS report for an IAV that had reappeared. The report observed that none of the individuals interviewed indicated that they would go back into OCRS to change a “Fully Compliant” IAV status when the IAV reappeared on the network. Rather, they stated that the practice was to address the IAV through a remediation action. The investigative team found that the interviews illustrated that Code 1153 personnel only addressed those IAVs in OCRS that had upcoming due dates. The report concluded that this could have contributed to the misunderstanding of OCRS reporting.

In his comments to the agency reports, Mr. McDuff stated his belief that evidence of malfeasance was destroyed before the investigation. According to the report, however, the

The President
January 15, 2015
Page 8 of 9

investigative team reviewed time-stamps of emails, dates of scan results, and the dates of information last reported in OCRS and found no evidence of manipulation.

The report observed that the investigation demonstrated how inadequate training and documentation for IA programs and personnel can lead to confusion. Specifically, the report noted that almost a year had passed since Division Newport released Standard Operating Procedures concerning IA functions. Finally, the agency noted that the lack of guidance requiring commands to amend prior OCRS compliance statuses, when an IAV reappears in subsequent scans, may have contributed to the confusion as well.

III. The Agency's Supplemental Report

On April 3, 2014, OSC requested additional information regarding the methodology used by the investigative team to calculate the number of IAVs in the nine scans, copies of the nine scan results themselves, and clarification of the reasons for the reappearance of IAVs. In response to OSC's request the agency provided a supplemental report on May 2, 2014. The supplemental report explained that the investigative team used Excel's "countif" function to tally the number of IAVs identified in the nine historic scans. The supplemental report also included the results of the redacted versions of the scans. Lastly, the supplemental report reiterated the reasons for the reappearance of IAVs in VARS scans after being reported as "Fully Complaint."

IV. Actions Taken

On September 29, 2014, OSC requested an update regarding the actions taken by Division Newport. On November 5, the agency responded to OSC's request and explained that while no corrective actions were deemed necessary, Division Newport has taken, or plans to take, a number of actions to address the concerns highlighted by the investigation. First, a vulnerability manager was hired in March 2014. Second, new IA staff members will receive training in workflow processes and scanning methodology tools. The agency indicated that vulnerability scanning methodologies are changing to accommodate the use of a new DOD mandated scanning environment. As a result, the Defense Information Systems Agency is providing free, online training that all new users must undergo in order to be granted access.

Third, with the migration to the new DOD mandated scanning and assessment suite, operation of the scanning is no longer an IA function but is now under the purview of the Operations Branch and is conducted by government employees rather than contractors. Under the new paradigm, IA handles the configuration, frequency, and oversight of the scanning under the direction of the vulnerability manager. In addition, contractors are under a separate security-based contract with a different company to provide separation of duties and to avoid conflicts of interests. Lastly, the Vulnerability Management Plan and the Standard Operating Procedures will be updated by February 1, 2015, to reflect the new scanning and assessment tool as well as the resulting change in process and workflow.

The Special Counsel

The President
January 15, 2015
Page 9 of 9

V. The Special Counsel's Findings

I have reviewed the original disclosure, the agency reports, and Mr. McDuff's comments. I acknowledge Mr. McDuff's objections to the agency's reports. Nevertheless, I find that the actions taken or soon to be taken by Division Newport adequately address his concerns. These actions include ensuring that the operation of the scanning is conducted by government employees rather than contractors, providing training to new personnel, and updating written policies and procedures. Based on my review, I have determined that the reports contain all of the information required by statute and that the findings appear to be reasonable.

As required by 5 U.S.C. § 1213(e)(3), I have sent copies of the unredacted reports and Mr. McDuff's comments to the Chairmen and Ranking Members of the Senate and House Committees on Armed Services. I have also filed copies of the redacted report, supplemental report, and Mr. McDuff's comments in our public file, which is available online at www.osc.gov. OSC has now closed this file.

Respectfully,



Carolyn N. Lerner

Enclosures