

Office of the Naval Inspector General

OSC DI-13-2697

NAVINGEN 201301997

Report of Investigation

16 January 2014

**NAVAL UNDERSEA WARFARE CENTER DIVISION NEWPORT,
NEWPORT, RHODE ISLAND**

**INFORMATION ASSURANCE VULNERABILITY ALERTS MITIGATION AND
REPORTING**

Table of Contents

Preliminary Statement.....	4
Introduction.....	5
Summary of Findings and Conclusions.....	6
Information Leading to the OSC Tasking.....	7
Description of the Conduct of the Investigation.....	8
Timeline of Events.....	10
Background Information.....	12
Roles and Responsibilities	12
Applicable IAVA Standards	14
NUWC Division Newport Vulnerability Management Plan	15
Remediation Process Standard Operating Procedure	20
Information Assurance Vulnerability Management (IAVM)	23
NUWC Division Newport's IAVM Program	23
IAVM Programmatic Risk Reduction	26
NUWC Division Newport IAVM Organizational Challenges	27
Remediation Task Force	28
Vulnerability Manager Position Vacancy	28
IAV Scans Reviewed During This Investigation.....	29

Allegation One.....	31
<p>That Subject 1, Information Assurance Manager, Naval Undersea Warfare Center Division Newport, Newport, Rhode Island, between March and April 2013, failed to mitigate known information assurance vulnerabilities, in violation of SECNAV M-5239.1, section 2.4.9. (Not substantiated).</p>	
Allegation Two.....	31
<p>That Subject 2, Remediation Manager, Naval Undersea Warfare Center Division Newport, Newport, Rhode Island, between March and April 2013, failed to mitigate known information assurance vulnerabilities, in violation of NUWC Division Newport Vulnerability Management Plan. (Not substantiated).</p>	
What the Complainant Contends	31
Findings	32
General Facts	32
Complainant-Conducted Scanning	33
Remediation Team E-mail Review	39
Inspections Oversight	40
Fleet Cyber Command Cyber Security Inspection	40
2012 NAVSEA Inspector General Triennial Command Inspection	41
Discussion and Analysis	43
Conclusion	46
Allegation Three.....	49
<p>That Subject 1, Information Assurance Manager, Naval Undersea Warfare Center Division Newport, Newport, Rhode Island, between March and April 2013, falsely reported information assurance vulnerabilities as being "Fully Compliant," in violation of SECNAV M-5239.1, section 2.4.9. (Not substantiated).</p>	
What the Complainant Contends	49
Complainant's Initial IAV and OCRS Reporting Concerns	50

Findings 50
 General Facts 51
 NUWC Division Newport OCRS Reporting Process 52
 NUWC Division Personnel Response to the Complainant 57
 Investigation Team’s Analysis of Alleged Misreported IAVs . 57
 Retroactive Compliance Reporting in OCRS 61
Discussion and Analysis 62
Conclusion 66
Observations 66
Actions Planned or Taken 67

Office of the Naval Inspector General

OSC DI-13-2697

NAVINGEN 201301997

Report of Investigation

16 January 2014

**NAVAL UNDERSEA WARFARE CENTER DIVISION NEWPORT,
NEWPORT, RHODE ISLAND**

**INFORMATION ASSURANCE VULNERABILITY ALERTS MITIGATION AND
REPORTING**

******* Preliminary**

Statement

1. This report is issued pursuant to a 3 July 2013 Office of Special Counsel (OSC) letter tasking the Secretary of the Navy (SECNAV) to conduct an investigation under 5 U.S.C. § 1213.

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

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

Introduction

4. This OSC tasking stems from a complaint OSC received concerning the mitigation and compliance reporting of Information Assurance Vulnerability Alerts (IAVAs) at Naval Undersea Warfare Center (NUWC) Division Newport, Newport, Rhode Island.

5. NUWC Division Newport provides the Department of the Navy (DON) with the technical foundation that enables the conceptualization, research, development, fielding, modernization, and maintenance of undersea systems¹. NUWC Division Newport is one of two subordinate divisions under the Naval Undersea Warfare Center. The Naval Sea Systems Command (NAVSEA) oversees the two NUWCs. NAVSEA is the largest of the Navy's five system commands.²

6. For the purpose of this investigation, an Information Assurance Vulnerability (IAV) is a software vulnerability that an attacker can exploit, potentially gaining unauthorized access to sensitive information. An IAV can affect one asset or numerous assets, based on software and hardware configurations. Because of this risk, the Department of Defense (DoD) has mandated that all activities scan their information technology (IT) networks and remediate all vulnerabilities³. DoD promulgates IAVs notifications and provides remediation actions to activities under its purview. These notifications carry specific compliance deadlines based on an IAV's amount of risk.

7. Because not all IAVs pose the same amount of risk, DoD categorizes IAVs into three categories⁴. Information Assurance Vulnerability Alerts (IAVAs) are considered the most serious IAVs, and pose the greatest risk of exploitation. IAVAs have the shortest compliance timelines and undergo the greatest

¹ <http://www.navsea.navy.mil/nuwc/newport/default.aspx>.

² <http://www.navsea.navy.mil/AboutNAVSEA.aspx>.

³ Navy Cyber Defense Operations Command (NCDOC) Communication Tasking Order (CTO) 11-16.

⁴ Listed successively from greatest risk to lowest risk, the three categories are: (1) Information Assurance Vulnerability Alerts (IAVAs), (2) Information Assurance Vulnerability Bulletins (IAVBs), and (3) Information Assurance Vulnerability Technical Advisories (IAVTs). Source: CJCSM 6510.01.

scrutiny by DoD. Commands are required to remediate IAVAs found on any vulnerable asset within 21 days of initial notification from DoD.

8. The OSC Complaint alleged that IAV scans conducted at NUWC Division Newport revealed "over 2,000 unmitigated IAVAs, 300 of which were high risk vulnerabilities." The complaint further alleged "at least eleven (11) high-risk IAVAs were being misrepresented as 'Fully Compliant' in the Online Compliance Reporting System (OCRS) without actually being fixed." The complainant also alleged that the failure to mitigate these IAVAs could result in access and manipulation of "hundreds of IT [Information Technology] devices, which pose a threat to the safety of unclassified and classified information concerning naval research and development."

9. After reviewing the complaint, OSC concluded that there is a "substantial likelihood" that the complainant's information may disclose gross mismanagement and a substantial and specific danger to public safety. OSC did not elaborate on any factual details underlying their "substantial likelihood" determination.

Summary of Findings and Conclusions

10. This report addresses the following three allegations:

Allegation One: That Subject 1, Information Assurance Manager (IAM), Naval Undersea Warfare Center Division Newport, Newport, Rhode Island, between March and April 2013, failed to mitigate known information assurance vulnerabilities, in violation of SECNAV M-5239.1, section 2.4.9. (Not substantiated).

Allegation Two: That Subject 2, Remediation Manager (RM), Naval Undersea Warfare Center Division Newport, Newport, Rhode Island, between March and April 2013, failed to mitigate known information assurance vulnerabilities, in violation of NUWC Division Newport Vulnerability Management Plan. (Not substantiated).

Allegation Three: That Subject 1, Information Assurance Manager, Naval Undersea Warfare Center Division Newport, Newport, Rhode Island, between March and April 2013, falsely reported information assurance vulnerabilities as being "Fully Compliant," in violation of SECNAV M-5239.1, section 2.4.9. (Not substantiated).

Information Leading to the OSC Tasking

11. In its tasking letter, OSC identified a single complainant, Mr. Jeffrey MCDUFF. OSC representatives stated that the complainant consented to the public release of his name. In this report, we refer to Mr. MCDUFF as the "complainant."

12. The complainant was a civilian IT Specialist, specializing in Information Security (INFOSEC)⁵. The complainant identified himself as a Certified Information Systems Security Professional (CISSP) within his e-mail signature block.⁶ The complainant worked within NUWC Division Newport's Physical Operations and Support Office. At NUWC Division Newport, Information Assurance (IA) functions fell under the Physical Operations and Support Office. Subject 1, the Division's IA Manager (IAM), was also located in the Physical Operations and Support Office.

13. According to the complainant, in the spring of 2013, his supervisor tasked him to support the Division's IA program. On 27 March 2013, Subject 1, IAM provided the complainant guidance regarding the IA support tasking. Specifically, Subject 1, IAM, told the complainant: "as far as the [IA] vulnerability management tasks... I'd like you to get trained up on our local processes so that you can step in and spread out the workload so we have more coverage on the

⁵ Information Security or INFOSEC is the system of policies, procedures, and requirements to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security. Source: DoDM 5200.01-V4, February 24, 2012.

⁶ CISSP certification is a professional certification credential in the field of information security. CISSPs are information assurance professionals who define the architecture, design, management and/or controls that assure the security of business environments. <https://www.isc2.org/CISSP/Default.aspx>.

the enterprise scanning.⁷” This assignment evolved into the scanning of the B3-COI [Boundary 3 Community of Interest]⁸ network on/around 3 April 2013.

14. The complainant was terminated from NUWC Division Newport on 15 April 2013.⁹

Description of the Conduct of the Investigation

15. SECNAV referred OSC’s 3 July 2013 tasking letter to the Office of the Naval Inspector General (NAVINSGEN) for investigation. NAVINSGEN assigned case number 201301997 to the matter, and forwarded the complaint to the Naval Sea Systems Command (NAVSEA) on 10 July 2013. NAVINSGEN directed the NAVSEA Inspector General (NAVSEAINSGEN) to conduct an investigation with collaboration and support from the U.S. Fleet Cyber Command Inspector General. In this report, the term “investigation team” describes the individuals from NAVSEAINSGEN tasked to investigate this complaint.

16. The investigation team focused on the detection, remediation, and compliance reporting requirements of IA Vulnerabilities (IAVs) on the B3-COI network at NUWC Division Newport. During the complainant’s interview with the investigation team, the complainant identified the B3-COI as the network he was responsible for scanning. These scanning responsibilities occurred between 27 March 2013 and 15 April 2013. The complainant stated that it was the B3-COI network where “over 2,000 unmitigated IAVAs, 300 of which were high risk vulnerabilities,” resided. It was also the B3-COI where the complainant alleged that “at least eleven (11) high-risk IAVAs

⁷ E-mail of 27 March 2013 from Subject 1, IA Manager to the complainant, 27 March 2013.

⁸ B3-COI, or the Boundary 3 Community of Interest, is a server arrangement that creates a boundary between the Navy Marine Corps Internet (NMCI) and communities of interest. NMCI is the Navy’s shore-based enterprise internet network. Communities of interest are a grouping of systems and users that utilize and share a common interest that can transcend organizational boundaries. This provides security between the community of interest and the NMCI network. Source: NMCI Master Abbreviations, Acronyms and Terms: https://www.homeport.navy.mil/about/downloads/master_glossary_of_acronyms.pdf

⁹ E-mail of 29 April 2013 from (name redacted) copying the complainant.

were being misrepresented as 'Fully Compliant' in the OCRS without actually being fixed." As a result, this investigation team focused its investigation on the operation of the B3-COI network, between the dates of 27 March 2013 and 15 April 2013.

17. The investigation team conducted interviews, collected documents, utilized Subject Matter Experts (SMEs), and drafted the report of investigation. During the investigation, the team conducted seven interviews, which included the complainant, witnesses, and subjects. Additionally, the investigation team had the Navy's Global Network Operations Center extract e-mail files from government computers assigned to the complainant and subjects. The team reviewed these e-mail files for evidence during the course of this investigation.

18. The investigation team obtained and reviewed nine historic IAV scan results for NUWC Division Newport's B3-COI networks. These scans represented the only scans available during the period in question. These scans were retrieved from Subject 2's, Remediation Manager, and the complainant's computers. These scans were conducted between 22 March 2013 and 18 April 2013. The complainant was assigned B3-COI scanning responsibilities between 27 March 2013 and 15 April 2013.

19. In order to eliminate any potential claim of not reviewing all networks at NUWC Division Newport, the investigation team also reviewed scan results for both the Division's Research Development Testing and Evaluation (RDT&E) network¹⁰ and a stand-alone enclave network¹¹. These scan results provided a representative sample for all network types at NUWC Division Newport. The investigation team also reviewed NUWC Division Newport's entries in the Navy's IAV compliance tracking database, the OCRS.

¹⁰ An RDT&E network is associated with a lab. A lab is a group of computers physically or virtually combined or connected for some common purpose. Some of the computers might be connected to a network and some of the computers might be stand-alone. The network to which the computers are connected might be a special internal network or the RDT&E network, which provides intra-Division connectivity and internet access.

¹¹ An enclave is a collection of computing environments connected by one or more internal networks under the control of a single source: SECNAV M-5239.1.

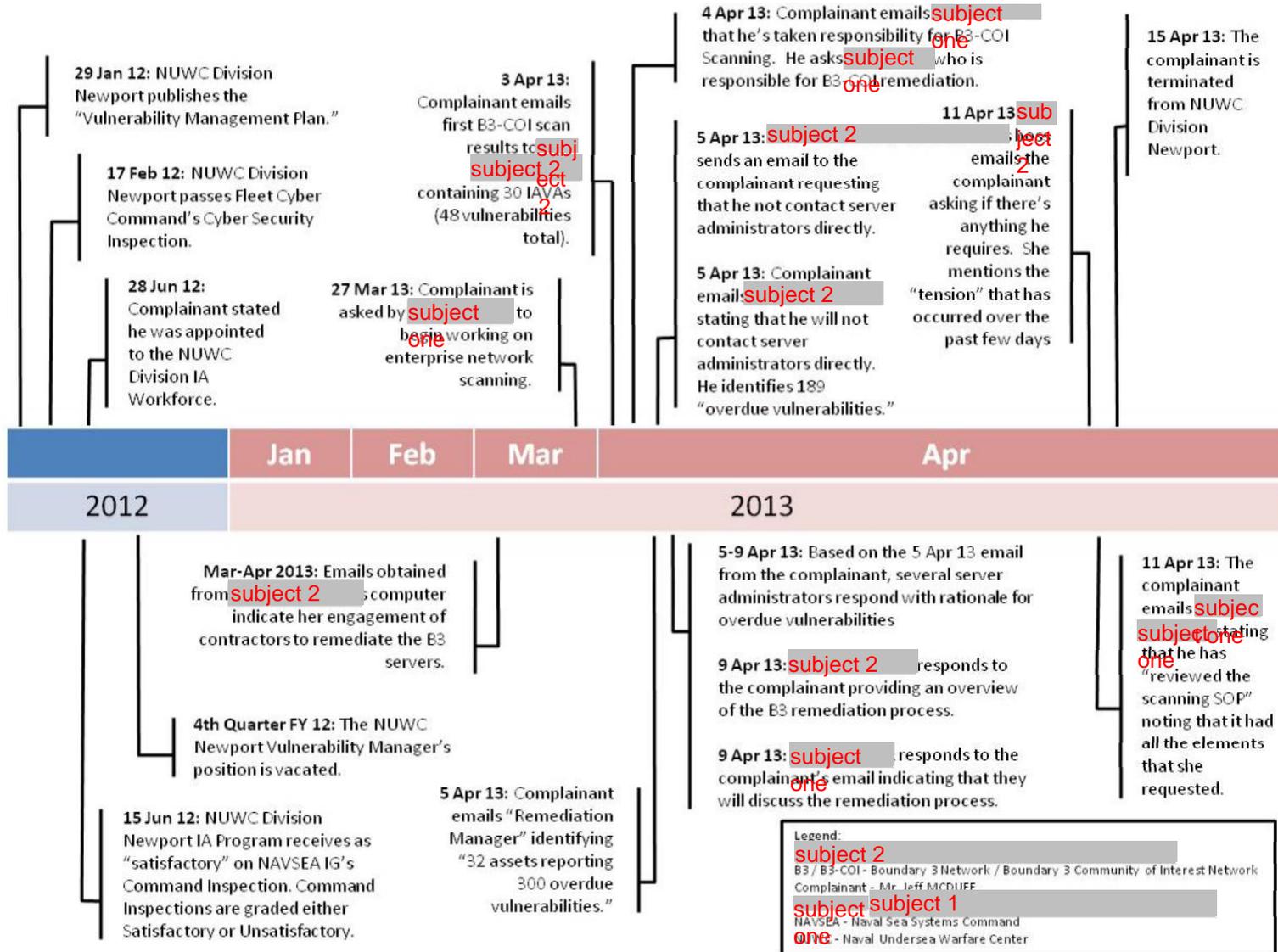
20. During the week of 26-29 August 2013, the investigation team conducted witness and subject interviews at NUWC Division Newport. During this time, the investigation team was able to review scan results and discuss with witnesses the local IAV process for scanning, remediating, and reporting compliance.

21. During this investigation, NAVINSGEN submitted three extension requests to OSC. The first request, dated 14 August 2013, was due to delays in receiving historical IAV scan results from NUWC Division Newport. OSC approved the first request with a new due date of 3 November 2013. NAVINSGEN sent the second request on 1 October 2013. This request was due to the tragic events that occurred at NAVSEA Headquarters' Building 197 at the Washington Navy Yard on 16 September 2013. OSC approved this second request by granting an extension to 6 January 2014. The third request was submitted on 23 December 2013 due to General Counsel and Secretary of the Navy unavailability until the first half of January 2014. OSC approved this third request by granting an extension until 31 January 2014.

Timeline of Events

22. In order to provide a consolidated presentation of the events pertinent to this investigation, a timeline is included on the following page. This timeline covers events ranging between the initial publishing of NUWC Division Newport's Vulnerability Management Plan, to the complainant's termination on 15 April 2013. See Figure 1 on the following page.

Figure 1: Timeline of events between January 2012 and April 2013.



Background Information

23. To facilitate a better understanding of the evidence and circumstances associated with the complainant's allegations made to OSC, and to facilitate a more knowledgeable assessment of this investigative report, it is important to understand certain background information that affected the IAV program at NUWC Division Newport. The following sections address DoD and DON IA roles and responsibilities, applicable DON standards and policies, the Division's IAV Management (IAVM), programmatic risk reduction efforts, and a discussion of the organizational challenges that affected the IAVM program.

Roles and Responsibilities

24. Within DoD, the U.S. Cyber Command¹² has the responsibility to plan, coordinate, integrate, synchronize, and conduct activities to direct the operations and defense of information networks.¹³ Prior to the stand up of U.S. Cyber Command, the Joint Task Force Global Network Operations (JTF-GNO) conducted DoD's offensive and defensive cyber operations.¹⁴ U.S. Cyber Command inherited the responsibility for identifying and mitigating threats to the DoD information network from JTF-GNO.¹⁵

25. The U.S. Fleet Cyber Command (Fleet Cyber Command) is under the operational control of U.S. Cyber Command. Part of Fleet Cyber Command's mission is to execute cyber missions as directed; as well as, to direct, operate, maintain, secure, and defend the Navy's portion of the Global Information Grid (GIG).

26. Subordinate to Fleet Cyber Command is the Naval Cyber Defense Operations Command (NCDOC) and the Naval Network Warfare Command (NETWARCOM). NCDOC provides oversight of vulnerability scanning and reporting, while NETWARCOM provides directives on how to mitigate IAVs. Specific agency responsibilities are discussed on the following page.

¹² U.S. Cyber Command is subordinate to U.S. Strategic Command. U.S. Strategic Command is one of the nine Unified Combatant Commands under the Department of Defense. Source: <https://www.cybercom.mil>.

¹³ http://www.stratcom.mil/factsheets/Cyber_Command/.

¹⁴ <http://www.defense.gov/News/NewsArticle.aspx?ID=60755>.

¹⁵ SECNAVINST 5239.3B 6.d.(1), 17 June 2009.

a. NCDOC is responsible for reporting incidents and associated analytical results to the U.S. Cyber Command.¹⁶ NCDOC is also responsible for releasing IAV information to Navy activities. NCDOC provides oversight of Navy activities IAV compliance via its OCRS. NCDOC requires Navy activities to keep IAV scan results for a minimum period of 90-days. NCDOC will periodically request scan results from selected commands for review.¹⁷

b. NETWARCOM is responsible for operating the Navy's networks to achieve effective command and control through optimal alignment, common architecture, mature processes and functions, and standard terminology.

27. NUWC Division Newport separates IA and remediation responsibilities between two offices (referred to as "Codes"). Code 1153 provides IA functions to include network IA vulnerability scanning and compliance reporting. Code 1142, the Remediation Team, is responsible for fixing identified vulnerabilities through the remote deployment of security patches, coordination with server administrators, and providing security configuration settings for centrally managed, networked computer systems.

28. Subject 1, within Code 1153, is the Information Assurance Manager (IAM) for NUWC Division Newport. Her 14 September 2010 appointment letter, signed by the Commander of NUWC Division Newport, included the following responsibilities:

a. "Developing and maintaining an IA program that identifies architecture, IA requirements, IA objectives and policies, IA Personnel, and IA processes and procedures."

b. "Ensuring that Compliance monitoring occurs, and review the results of such monitoring, notifying the cognizant [authority] of significant findings."

¹⁶ SECNAVINST 5239.3B 6.d.(2), 17 June 2009.

¹⁷ CTO 11-16A.

29. Subject 2, within Code 1142, is the Remediation Manager (RM) for NUWC Division Newport. Subject 2's responsibilities, according to the Division's Vulnerability Management Plan, include the remote deployment of security patches and security configuration settings to centrally managed, networked computer systems. There is no formal appointment letter assigning Subject 2, remediation duties.

Applicable IAVA Standards

30. Conducting this investigation required a review of the SECNAV's Information Assurance Manual (SECNAV MANUAL), one Navy Order (responsible Command order), and local NUWC Division Newport policy and corresponding procedures. The Navy standards set forth requirements for NUWC Division Newport to scan, remediate, and report IAV compliance. Specifically, the SECNAV's Information Assurance Manual sets broad policy and requirements, while NETWARCOM's Communication Tasking Orders (CTO) provided specific requirements for executing scans and reporting results. NUWC Division Newport's Vulnerability Management Plan and Remediation Process Standard Operating Procedure outlined the local policies and procedures required to execute the SECNAV and NETWARCOM requirements.

31. The SECNAV Manual, SECNAV M-5239.1 (November 2005) "Department of the Navy Information Assurance Manual," addresses the roles and responsibilities for the DON IA workforce in receiving, complying, and reporting IAVAs.

a. Section 2.4.9. states IA Managers are responsible for:

"the information assurance program within a command, site, system, or enclave. The IAM is responsible for local IA Command Authority and DAA (Designated Approval Authority) for ensuring the security of an IT [Information Technology] system, and that it is approved, operated, and maintained throughout its lifecycle in accordance with IT system security certification and accreditation.

b. Section 4.8.2. states IAVM actions:

"shall be addressed and compliance reported within the timeframe allotted by DoD."

32. NETWARCOM's Communication Tasking Order (CTO) 11-16 implements the SECNAV Manual's requirements [timeframe allotted by DoD] for IAVM scanning, remediation, and reporting, specifically:

a. The CTO states:

"SECURE CONFIGURATION COMPLIANCE VALIDATION INITIATIVE (SCCVI) SCANS MUST BE COMPLETED AND REMEDIATED AT A MINIMUM EVERY (30) DAYS USING RETINA SCANNING TOOLS WITH ALL AUDITING AND AGENT.BTZ ENABLED." [eEye's Retina scanner is the approved network vulnerability scanning tool employed by DoD.]

b. For the B3-COI network, the CTO requires:

"PERFORM MONTHLY SCCVI SCANS ON NIPRNET AND SIPRNET NETWORKS.... SCAN RESULTS ARE TO BE ARCHIVED FOR A MINIMUM OF 90 DAYS AS NCDOC WILL PERIODICALLY REQUEST SCAN RESULTS FROM SELECTED COMMANDS FOR REVIEW."

c. Lastly, the CTO mandates:

"UNITS/COMMANDS MUST REPORT TOTAL NUMBER OF AFFECTED ASSETS (NUMBER OF ASSETS CONNECTED TO THE NETWORK) AND TOTAL NUMBER OF ASSETS CORRECTED (NUMBER OF ASSETS SCANNED) [in accordance with] THIS CTO."

NUWC Division Newport Vulnerability Management Plan

33. NUWC Division Newport's Vulnerability Management Plan (VMP), was signed by Subject 1, in her capacity as the IAM, as appointed by the Division's Commander. The most current version of the VMP is dated 30 May 2012. The first version of the VMP was dated 29 January 2012.

34. The VMP contains polices and guidelines necessary to ensure the Division's systems are configured in compliance with DoD and DON security mandates. The VMP outlines scanning and remediation positions and responsibilities, the local scanning policy, the disconnect policy for non-IAV compliant systems, as well as local and higher headquarter reporting requirements.

35. The VMP describes the Division's scanning operations with regards to centrally managed systems, which include the B3-COI networks:

"centrally managed systems are scanned at least daily using the SCCVI tool [eEye Retina Tool], surpassing the Communications Tasking Order requirement for monthly scans."

36. The VMP outlines a compliance enforcement policy:

"Networked assets noncompliant with security configuration pose a threat to both SIPRnet and NIPRnet DoD Global Information Grids [GIG] (networks). Thus, systems with GIG connectivity are removed [by Code 1153 personnel] from the network when they do not meet the compliance deadlines for both IAV and Non-IAV vulnerabilities. When non-compliant, disconnected systems reach IA compliance, they may be reconnected to the network."

37. The VMP describes the local vulnerability IAV monitoring. This encapsulates the Division's locally developed Vulnerability Analysis and Remediation System (VARS), which the IA workforce uses to monitor their respective networks for IAV scan results and compliance. Specifically, the VMP states:

"Local reporting is accomplished using a web front end [VARS] that automatically imports scan data from the vulnerability scanners [eEye Retina Scanner] once scans, run at least once daily for all networks, are completed. IA work force have access to the

database website, but only for systems in their respective labs, due to the sensitive nature of scan result data. The IAM staff [Code 1153 IA personnel] manages access to the web database, and ensures only qualified IA workforce personnel, certified in writing to the positions, are granted access.”¹⁸

38. Additionally, the VMP describes the reporting of IAVM statuses to higher headquarters. Specifically:

“NUWC Division Newport is required to report IAVM status for new IAVs, as released by the Navy Cyber Defense Operations Command, within the prescribed time constraints.... The reporting tool for Navy commands to report IAVM compliance is the Online Compliance and Reporting System (OCRS). NUWC Division Newport must first acknowledge new IAVs within the prescribed time constraints [to NCDOC via OCRS], typically 24 hours. After acknowledgement, NUWC Division Newport must report compliance of pending IAVs before the prescribed due dates. If a due date cannot be met, a mitigation (extension) request must be sent with enough lead time to ensure approval of the mitigation request before the IAV due date.”

39. The VMP captures the roles and responsibilities at NUWC Division Newport.

a. For the Information Assurance Manager (IAM): “The NUWC

Division Newport IAM is responsible for all policy, procedures, and

¹⁸ Although Subject 2, RM, was not formally appointed by the Commander of NUWC Division Newport, she had the requisite access to review IAV scan results, as verified by scan results obtained from her government e-mail files. Given the fact that Subject 2, RM, was properly hired into her current position, she was qualified to execute the requirements of the Remediation Manager).

operations for all facets of IA at Division Newport and its detachments. The IAM directs the Vulnerability Manager to implement the IAVM program. The IAM briefs IAVM status to the NUWC Chief Information Officer, Department Heads, Technical Director, and the Commanding Officer.

b. For the Vulnerability Manager:

"The NUWC Division Newport Vulnerability Manager is responsible for the full lifecycle of the IAVM process." The Vulnerability Manager's responsibilities include:

- "Maintains DoD-approved systems and software, in alignment with SCRI [Secure Configuration Remediation Initiative], which remotely deploys security patches to centrally managed, networked systems."
- "Coordinates with IAOs [Information Assurance Officers] to ensure standalone systems and systems in standalone enclaves are as IA compliant as the centrally-managed, networked systems."
- "Ensures Program of Record (POR) Systems are identified, as IA compliance responsibility for these systems lies with the respective Program Executive Office (PEO)."
- "Manages IAV Status Reporting. Ensures Information Assurance Officers (IAOs) and System Administrators receive daily status of vulnerability scans. Provides IAOs and System Administrators due dates for IAVs. Ensures IAVs are reported before the due date in the

Navy's Online Compliance and Reporting System (OCRS)."

- "Manages disconnections of networked systems due to IA noncompliance and provides a process to reconnect systems once determined to be IA compliant."

c. For the Remediation Manager:

"The NUWC Division Newport Remediation Manager is responsible for remote deployment of security patches and security configuration settings to centrally managed, networked computer systems." The Remediation Manager:

- "Maintains DoD-Approved systems and software, in alignment with SCRI, which remotely deploys security patches to centrally managed, networked systems. The Remediation Manager manages and maintains tools, such as Microsoft's Windows System Update Server (WSUS) suite, ensuring the tools are kept current with the latest patches and configured to successfully deploy patches to the maximum number of remote hosts."
- "Coordinates with Server Administrators to capitalize on Directory Service tools, such as Microsoft Active Directory Group Policy, to implement secure configuration settings, such as Windows registry settings."
- "Provides a patch repository offering IAWF [Information Assurance Workforce] access to IAV patches."

40. The VMP outlines the disconnection policy for deficient assets at the Division. System disconnect occurs when a machine fails to meet IAV and non-IAV compliance. Specifically:

“Networked assets noncompliant with security configuration requirements pose a threat to both SIPRNet and NIPRNet DoD Global Information Grids (GIG) [computer networks]. Thus, systems with GIG connectivity are removed from the network when they do not meet compliance deadlines for both the IAV and Non-IAV vulnerabilities. When noncompliant, disconnected systems reach IA compliance, they may be reconnected to the network.”

41. The VMP also outlines the IA vulnerability compliance reporting requirements, both locally and to higher headquarters. With respect to higher headquarter reporting, the plan states:

“NUWC Division Newport is required to report IAVM status for all new IAVs, as released by [NCDOC] within the prescribed time constraints... The reporting tool for Navy commands to report IAVM compliance is the [OCRS]. NUWC Division Newport must first acknowledge new IAVs within the prescribed time constraints, typically 24 hours. After acknowledgement, NUWC Division Newport must report compliance for pending IAVs before the prescribed due dates. If a due date cannot be met, a mitigation (extension) request must be sent with enough lead time to ensure approval of the mitigation request before the due date.”

Remediation Process Standard Operating Procedure

42. NUWC Division Newport’s IT Standard Operating Procedures (SOP), dated 2 September 2012, outlines the VARS system color-coding for IAVs identified during network scans. Further, the scope for remediation captures the B3-COI Production,

Development, Foreign, and SecureNPT domains. The SOP outlines the remediation process on the following pages.

“1. The process of remediation begins when a failed audit is found by the eEye¹⁹ Retina Network Security Scanner²⁰ on a specific system. This begins the timeline for remediation and potential disconnect.

2. The authoritative source to be used for tracking vulnerabilities will be the Vulnerability Analysis and Reporting System (VARS) tool. Stages of the timeline for the identification and remediation of vulnerabilities are tracked in VARS by three-color codes: Green, Orange and Red. ²¹

a. Green signifies the time period between which a vulnerability audit is created in Retina and 5 days prior to the due date. The number of days a host could be in this status is a factor of the lead time allowed between the release of the relevant audit item and the reporting due date.

b. Orange is a warning zone between Green and Red. A vulnerability coded in Orange is within 5 days of the relevant audit item's reporting due date. IAO's are advised to take note of systems with an Orange status as this may imply that automated means have been unsuccessful at delivering required updates.

¹⁹ “eEye” Digital Security was acquired by BeyondTrust in May 2012. eEye Digital Security product offerings included enterprise software, appliances and services to help organizations protect their IT assets.

<http://www.beyondtrust.com/NewsEvents/PressReleasesDetails/201/>

²⁰ eEye Digital Security's Retina Network Security Scanner is a vulnerability assessment application and enables the identification of IT exposures and prioritize remediation enterprise-wide.

<http://www.wideeyesecurity.com/datasheets/Retina-GOV-DS.pdf>.

²¹ VARS color-coding will automatically adjust based on the compliance-due date of the IAV that is set by NCDCC.

c. Red means that the vulnerability is now considered past due and must be remediated within 3 days or the affected host will be nominated for disconnect. VARS displays the number of days that each machine has been reporting non-compliance for each relevant audit item.

3. The Code 1142 Remediation Team will be responsible for remediating systems in Green and Orange status.

a. Automated methods that the Remediation Team may use include Windows Server Update Services (WSUS) and batch scripting processes.

b. Remediation by these automated methods will occur between the hours of 2200 and 0530.

c. Remediation may be attempted via Remote Desktop Connection (RDC) during working hours provided there are no users logged on to the affected host and it is available on the network.

d. Delivery of patches/updates via automated or manual means is limited to the following products:

i. Windows XP Professional SP3 and higher

ii. Microsoft Office 2003 and higher

iii. Adobe Reader

iv. Adobe Flash

v. Adobe Acrobat

vi. Mozilla Firefox

vii. Java JRE/DK

viii. Google Chrome

Updates to all other software, applications, and operating systems are the responsibility of the IAO.

4. Once a vulnerability reaches Red status, it then becomes the IAO's [Code 1153] responsibility to ensure the system is compliant prior to the disconnect date. At this time, all remediation via RDC by the Remediation Team will cease. Access to automated patching via WSUS and/or batch scripting will still be available, but is unlikely to be successful.

5. IAO's are responsible for daily monitoring of VARS for the compliance status of systems under their control."

Information Assurance Vulnerability Management (IAVM)

43. The NCDOD requires²² the Division to scan its networks for vulnerabilities, remediate any vulnerability, and then report scanning and remediation efforts into a centralized Navy database. This cyclical process of scanning, remediating, and reporting is referred to as IAVM. IAVM protects the security of DoD's Global Information Grid and reduces the risk of exploitation by an attacker.

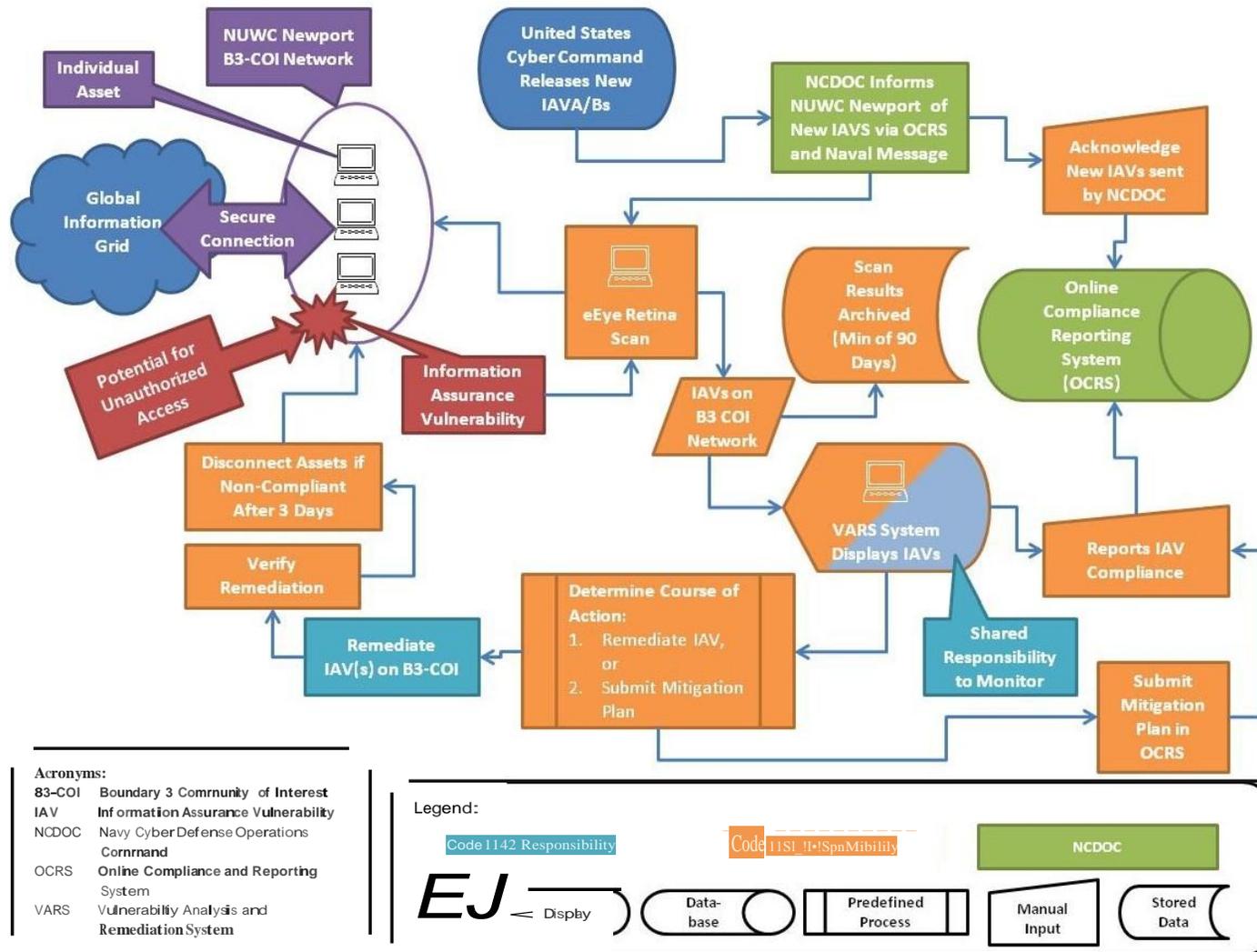
44. The following sections present the NUWC Division Newport IAVM program in detail, as well as discuss the programmatic risk reduction mechanisms in place for the Division's IAVM program.

NUWC Division Newport's IAVM Program

45. NUWC Division Newport has multiple computer assets divided into several separate networks. The diagram on the following page captures the processes and responsibilities at NUWC Division Newport for the scanning, remediating, and reporting of IAVs on the B3-COI network. See Figure 2 on the following page.

²² NCDOD CTO 11-16.

Figure 2: NUWC Division Newport 83-COI IAVM Process



46. An IAV has the potential to allow for unauthorized access to a secure network. As seen in Figure 2 on the previous page, U.S. Cyber Command issues IAVs to NCDOD. In turn, NCDOD will notify NUWC Division Newport that there is a new IAV requiring action. NCDOD provides this IAV notification via OCRS and Navy Message²³. NCDOD requires the Division's staff to acknowledge that it has received the IAV notification utilizing OCRS. Concurrently with the acknowledgement in OCRS, Code 1153 staff will update the eEye Retina scanner (the tool used to search the B3-COI network for the IAVs required to be remediated by NCDOD).

47. In order to ensure NUWC Division Newport is scanning and remediating IAVs, NCDOD requires the Division to report IAV compliance into its OCRS system. Compliance reporting in OCRS is a manual process, as the scanner will not automatically upload data into OCRS. OCRS tracks the number of unclassified and classified assets that are affected; corrected; implementing a permanent fix; with an approved mitigation plan; or, not compliant and does not have a mitigation plan or permanent fix.

48. Code 1153 conducts scans to detect IAVs on the Division's B3-COI network. The eEye Retina Scanner is the sole tool used by the Division to detect IAVs. The eEye Retina scans are conducted on a daily basis at NUWC Division Newport, surpassing NCDOD's monthly scan and remediation requirement. The eEye Retina scan data is automatically uploaded into the Division's Vulnerability Analysis and Remediation System (VARS) for viewing.

49. VARS is a locally developed system created by NUWC Division Newport personnel. VARS provides a graphic dashboard display of IAVs discovered during the Division's daily scans. It provides the Division Staff a color-coded (red/yellow/green) compliance indicator for each IAV discovered. This color-coding indicates the compliance timeframe required by NCDOD.

²³ Navy messages include NAVADMINS, which are Navy-specific administrative messages, and ALNAVs, which are messages that are directed to all Navy units and the Marine Corps. <http://www.public.navy.mil/bupers-npc/reference/Messages/Pages/default.aspx>.

50. Code 1153 and 1142 personnel use VARS to track IAVs scans, and collectively determine if an IAV can be remediated immediately. Code 1142 handles the remediation efforts. If a vulnerability cannot be immediately remediated due to the scope or remediation requirements, Code 1153 will submit a mitigation plan to NCDOC in order to afford the Division personnel more time to address the vulnerabilities. Code 1153 reports IAV compliance and submits mitigation plan requests in OCRS.

51. If a remediation action is not successful, the IAV will continue to reappear in subsequent daily scan results populated into VARS. If an IAV is not corrected after three days, or a mitigation plan is not submitted, the deficient asset will be disconnected from the B3-COI network remotely by Code 1153 personnel.

52. If NUWC Division Newport does not report IAV compliance in OCRS within the timeframe prescribed by NCDOC, it will receive a "delinquency message." NCDOC provides this delinquency message to the Division via Navy Message and through OCRS.

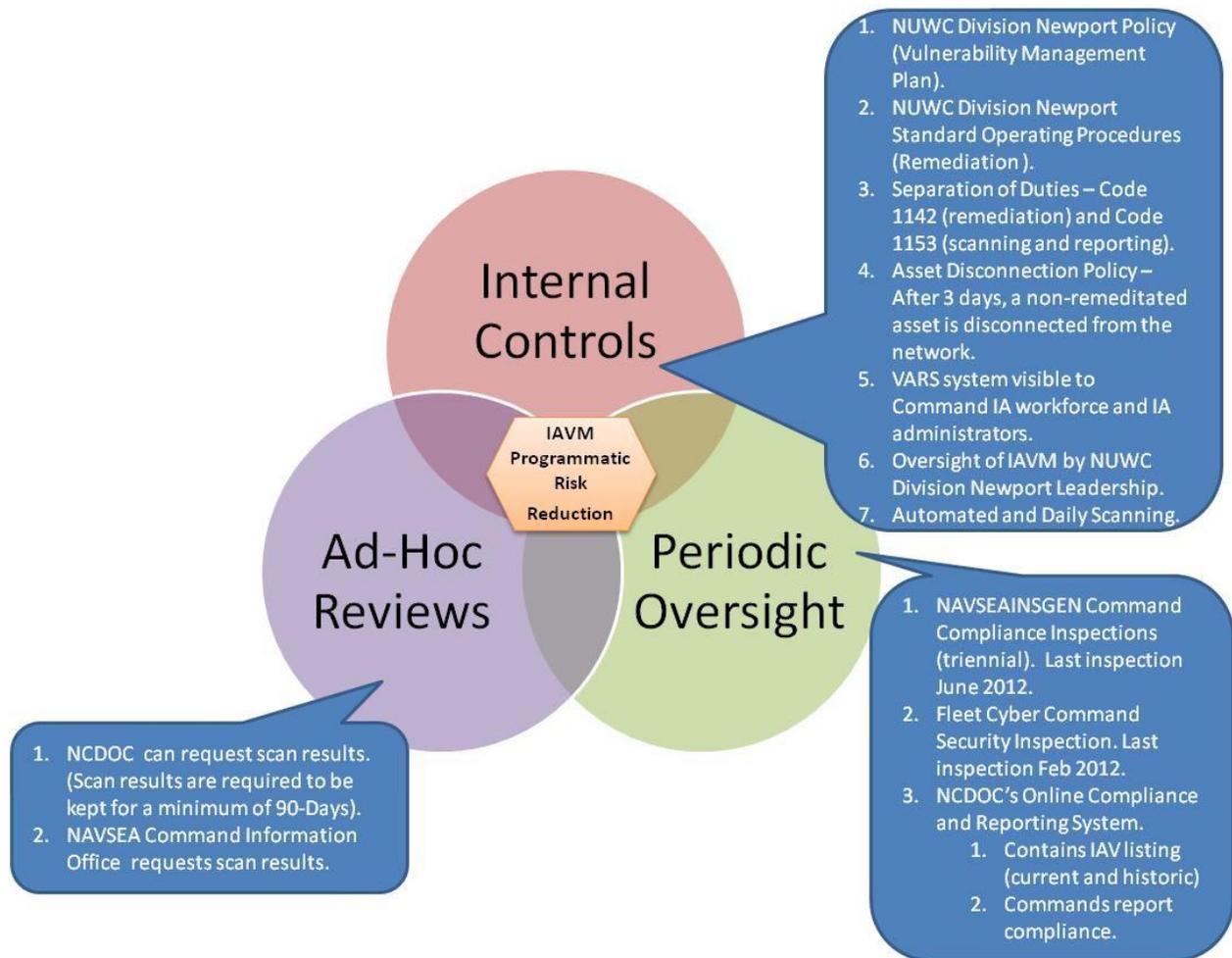
53. NUWC Division Newport's IAVM process will only work if the Division follows internal standard operating procedures and external policies. There are several types of controls in place to ensure IAVM compliance. These compliance mechanisms reduce the programmatic risk of the Division's IAVM program.

IAVM Programmatic Risk Reduction

54. This investigation found that the risk of programmatic deviations to the Division's IAVM program is addressed in three distinct areas. The first area, internal controls, consists of efforts to ensure Division staff accomplish assigned IAVM duties. The second, Command Oversight, consists of periodic higher-headquarter efforts to ensure NUWC Division Newport meet its IAVM responsibilities. The last, Ad-Hoc Reviews, consists of no-notice data calls for scan results. All three areas converge to ensure the Division institutes an effective IAVM program.

55. The following figure is a graphic representation of the IAVM programmatic risk reduction efforts undertaken by NUWC Division Newport. Additionally, it captures the oversight mechanisms utilized by higher-headquarters. Collectively, these efforts ensure Division personnel adhere to the IAVM process, reducing the risk to the network. See Figure 3 below.

Figure 3: IAVM Programmatic Risk Reduction



NUWC Division Newport IAVM Organizational Challenges

56. Prior to the complainant's assignment to conduct IAV scans of the B3-COI network, NUWC Division Newport experienced two separate IAVM organizational impediments. The first was a contract dispute that affected the contractors tasked to support

the Divisions IAVM program. The second challenge was the lack of a government Vulnerability Manager to oversee the IAVM Program. These challenges and the corresponding mitigation efforts are discussed in the following sections.

Remediation Task Force

57. In January 2013, a non-successful contract bidder protested the Division's newly awarded IT Support contract. According to those interviewed by the investigation team (complainant, witnesses, and subjects), IAV scanning and remediation were two tasks directly impacted by the contract protest.

58. Witnesses and subjects stated that the contract protest, coupled with the lack of a vulnerability manager, exacerbated difficulties with the scanning and remediation process. Because of the protest's impacts, the Division Information Technology/Information Assurance (IT/IA) workforce created the "Remediation Task Force" as a temporary solution to the lost contractor support.

59. On 22 January 2013, Subject 2 sent an e-mail to Division IT personnel, outlining the Remediation Task Force efforts, specifically:

a. Review VARS data daily for the network connected labs in your code.

b. Take or direct action to resolve any finding shaded in orange [from the VARS IAV scan spreadsheet]. See Figure 5 in Appendix D.

Vulnerability Manager Position Vacancy

60. Throughout the complainant's tenure of B3-COI IAV scanning, NUWC Division Newport's Vulnerability Manager position was vacant. NUWC Division Newport's Vulnerability Management Plan outlines the responsibilities for the Vulnerability Manager. The Vulnerability Manager is responsible for the "full life cycle" of the IAVM process, to include management of the "IAV status reporting" in OCRS, management of the disconnection

process for IA non-compliant systems, and the management of the scanning process. Specifically, the Vulnerability Manager was responsible for ensuring IA personnel received daily status of vulnerability scans, reporting IAV status in OCRS, and managing disconnects for noncompliant assets.

61. According to witness and subject testimony, the Division's Vulnerability Manager position has remained vacant since the 4th Quarter of Fiscal Year (FY) 2012. The lack of a government Vulnerability Manager caused the complainant, Witness 1, Witness 2 (contractors), and Subject 2, RM, to assume the vulnerability manager responsibilities at Subject 1's (IAM) request.

62. On 9 April 2013, the complainant identified his actions, in part, to have assumed the role of the Vulnerability Manager. See Figure 6 in Appendix D.

63. On 9 April 2013, Subject 2 responded to the complainant's e-mail, stating that the "absence of a vulnerability manager has been dealt with through daily conversation with Witness 1 and Witness 2 (contractors supporting Subject 1, IAM, in Code 1153) in order to maintain situational awareness of the B3 Compliance State." See Figure 7 in Appendix D.

IAV Scans Reviewed During This Investigation

64. This investigation required the review of historic scan results of the B3-COI network for the period in question. The following section discusses this investigation's scope of review of the Division's IAV scans.

65. NUWC Division Newport's policy was to scan its networks daily. Following the daily scans, the data was uploaded into VARS for review and action. The NCDOC required the Division to retain IAV scan records for a period of 90-days. NUWC Division Newport produced scan results of the B3-COI on a daily basis. As a result, 90-day old scan results were discarded as new scan results were generated, in accordance with NCDOC directives. This continual recycling of data within VARS, and the limited

retention requirements for B3-COI scan results, made it difficult for the investigation team to get the scan results for the period identified by the complainant.

66. The investigation team had to rely on scan results obtained from e-mail extractions on the subjects' and complainant's government computers. These scan results were analyzed and then discussed during interviews with the individuals responsible for conducting IAVM at the Division.

67. IAV scan results extracted from the subjects' and complainant's government computers contained historic IAV scan results for the Division's B3-COI network. Based on e-mail correspondence retrieved from the subjects' and complainant's computers, the investigation team independently confirmed the complainant did conduct IAV scans of the B3-COI network between 27 March 2013²⁴ and 15 April 2013. The following table contains the total scan results the investigation team retrieved from the complainant's IAV scanning tenure and reflects the IAV scans evaluated during this investigation. See Table 1 below.

Table 1: B3-COI Scans Reviewed During This Investigation.

Date of Scan	Retrieved From	Contents
22 March 2013	Subject 2, RM's E-mail Files	VARs Scan Results B3 COI
27 March 2013	Subject 2, RM's E-mail Files	VARs Scan Results B3 COI
3 April 2013 **	Complainant's E-mail Files	VARs Scan Results B3 COI
4 April 2013	Subject 2, RM's E-mail Files	VARs Scan Results B3 COI
5 April 2013 **	Complainant's E-mail Files	VARs Scan Results B3 COI
8 April 2013 **	Subject 2, RM's E-mail Files	VARs Scan Results B3 COI
9 April 2013	Complainant's E-mail Files	VARs Scan Results B3 COI
10 April 2013	Subject 2, RM's E-mail Files	VARs Scan Results B3 COI
18 April 2013	Subject 2, RM's E-mail Files	VARs Scan Results B3 COI

*** Indicates a complainant conducted scan.*

68. The investigation team corroborated the scan results with the testimony of those individuals responsible for scanning,

²⁴ E-mail of 27 March 2013 from Subject 1, IAM, to complainant assigning vulnerability scanning to the complainant. B3-COI was identified during the subjects', witnesses', and complainant's interviews.

reviewing the scan results, remediating any IAVs discovered, and reporting the IAV compliance state in OCRS.

69. It is important to note that the amount of IAVs found during each scan is not cumulative. For example, if one day's scan results reveal that there are 30 IAVAs, and the following day's scans has 40 IAVAs, it does not mean that there are 70 IAVAs on the network. Rather, the scan results show the IAVs that exist on the network during a snapshot in time. The variance in IAVs between each scan result indicated Division personnel were executing their assigned IAV remediation responsibilities.

Allegation One

That Subject 1, ND-05, Information Assurance Manager, Naval Undersea Warfare Center Division Newport, Newport, Rhode Island, between March and April 2013, failed to mitigate known information assurance vulnerabilities, in violation of SECNAV M-5239.1, section 2.4.9. (Not substantiated).

Allegation Two

That Subject 2, NT-04, Remediation Manager, Naval Undersea Warfare Center Division Newport, Newport, Rhode Island, between March and April 2013, failed to mitigate known information assurance vulnerabilities, in violation of NUWC Division Newport Vulnerability Management Plan. (Not substantiated).

What the Complainant Contends

70. The OSC tasking letter states that the complainant found over "2,000 unmitigated IAVAs, 300 of which were high-risk vulnerabilities." The investigation team assumed that the appearance of these alleged vulnerabilities would have occurred during the complainant's 27 March 2013 to 15 April 2013 B3-COI scanning tenure. Further, based on the complainant's assigned responsibilities, these alleged vulnerabilities would have only appeared during B3-COI scanning and not on any other network at NUWC Division Newport.

71. The complainant contended that the "failure to mitigate the IAVAs could result in access to, and manipulation of hundreds of IT devices, which pose a threat to safety of unclassified and classified systems concerning naval research and development."

Findings

72. The following findings of fact address the complainant's allegation that there were "2,000 unmitigated IAVAs, 300 of which were high-risk vulnerabilities" on the Division's B3-COI network. NCDOC categorizes IAVAs as the highest risk IAV; there is no separate category of "high-risk" IAVs.

General Facts

73. The complainant was only responsible for conducting IAV scans of the Division's B3-COI network. The investigation team's analysis is of the historic scan results, as well as the e-mails pertinent to the B3-COI IAV scanning. Additionally, all relevant testimony obtained during the course of this investigation is presented alongside other findings. Finally, the facts presented help to illustrate the business practices employed by the Division's employees responsible for scanning, remediating, and reporting IAV compliance.

74. The investigation team obtained and analyzed e-mail files from the complainant's and the two subjects' government computers. These e-mail files were pertinent to the complainant's scanning and subsequent concerns of the B3-COI network. The investigation team extracted and analyzed all e-mails regarding B3-COI network scans and the B3-COI scanning process from these three computers. The e-mails presented below also provide facts concerning the inter-office relationships between the subjects and the complainant.

75. Scan results analyzed by the investigation team found fewer than 300 IAVAs existed on the B3-COI network at any one time. For example, the complainant's scan results sent to the NUWC

Division Newport's IA staff only had 30²⁵ and 189²⁶ IAVAs. The number of IAVAs found during scans fluctuated, which indicated IA and Remediation teams were actively addressing the vulnerabilities. IAVs found on earlier scan results did not appear in subsequent scan results.

76. Testimonial evidence obtained during the 26-29 August 2013 site visit was included as corroborating facts to the information derived from the e-mail analysis. During the witness and subject interviews, all of the individuals responsible for B3-COI IAV scanning and remediation independently stated that they had never seen 2,000 IAVAs on the B3-COI network during a single daily scan result.

77. Finally, evidence from prior inspections and efforts related to the Division's IAVM program are included to provide an overview of the business practices exercised by NUWC Division Newport employees.

Complainant-Conducted Scanning

78. In his 1 August 2013 telephone interview with the investigation team, the complainant stated that his assignment to the B3-COI network scanning duties was due, in part, to the lapse in contractor support. Specifically:

a. Prior to his involvement, scanning was being executed only by contractors.

b. NUWC Division Newport had experienced contractual issues, jeopardizing the IA scanning function.

c. The complainant's appointment to the IA scanning team was to ensure program continuity.

79. The following paragraphs discuss e-mails sent between the complainant, the two subjects, and several witnesses. The e-mails are presented in detail in order to describe the

²⁵ E-mail of 3 April 2013 from complainant to Subject 1 . See Figure 10.

²⁶ E-mail of 5 April 2013 from complainant to Subject 2 . See Figure 16.

chronology of events concerning the complainant's B3-COI IAV scanning duties.

80. On 27 March 2013, Subject 1, IAM, sent the complainant an e-mail. Under a subject line of "RE: Time Cards, "Subject 1, IAM, tasked the complainant to begin working with the support contractors to conduct the enterprise network scanning. See Figure 8 in Appendix D.

81. On 3 April 2013, the complainant e-mailed Subject 2, RM. This was the first e-mail sent by the complainant where he identified "overdue vulnerabilities." In his e-mail, the complainant attached a spreadsheet that listed the overdue vulnerabilities found in VARS. The complainant made no mention of "high risk vulnerabilities." See Figure 10 in Appendix D.

82. The attachment from the complainant's 3 April 2013 e-mail, subject "Overdue Audits 04_03_13.xlsx," contained 22 unique IAVAs. In total, there were 30 assets with IAVAs, 2 assets with IAVBs, and 1 asset with an IAVT. See Figure 11 in Appendix D.

83. On 4 April 2013, the week following the initial assignment of enterprise scanning, a series of e-mails was sent between the complainant, Subject 1, IAM, and Subject 2, RM.

a. First, the complainant sent an e-mail to Subject 1, IAM, subject "B3COI Coverage and Overdue IAVAs." In this e-mail, the complainant initially presented IAVs to Subject 1, IAM, which he believed to have not been mitigated. The complainant made no mention of "high risk vulnerabilities." See Figure 12 in Appendix D.

b. In response to the complainant's e-mail, Subject 1, IAM, asked the complainant several questions about the B3-COI scans and IAVAs he presented. Subject 1, IAM, referred the complainant to Subject 2, RM, for B3-COI remediation issues. Subject 1, IAM, discussed "deferrals," which are mitigation actions that have been delayed with an approved plan vetted through OCRS, and approved by NCDOD. See Figure 13 in Appendix D.

c. Subject 1, IAM, then e-mailed Subject 2, RM. This e-mail confirmed that Subject 2, RM, was the POC [point of contact] responsible for B3-COI remediation. Subject 1, IAM, further stated that she would relay this information to "Jeff" [the complainant]. See Figure 14 in Appendix D.

d. Finally, Subject 2, RM, responded to the complainant's e-mail, stating that she would review the IAV findings presented in the 3 April 2013 e-mail, subject: "Overdue Audits 04_03_13.xlsx." Subject 2, RM, requested the complainant not contact the server administrators directly. Specifically, Subject 2, RM, stated "neither you [complainant] nor I [Subject 2, RM] have the authority to direct SAs [Server Administrators] or assign them tasking." Based on the statement made by Subject 2, RM, it appeared that the complainant had gone directly to SAs for remediation actions prior to her e-mail. See Figure 15 in Appendix D.

84. On 5 April 2013 at 1157, the complainant responded via e-mail to Subject 2, RM's request not to contact the Server Administrators. The complainant stated that the number of overdue IAVAs has increased to 189. See Figure 16 in Appendix D.

85. On 5 April 2013 at 1539, the complainant sent Subject 2, RM, an e-mail explaining, "32 assets [network connected machines with unique Internet Protocol (IP) addresses] are reporting 300 overdue vulnerabilities" in the Division's VARS. The complainant made no mention to "high risk vulnerabilities." Four assets, identified by their unique IP addresses, accounted for over 75% of the IAVs found by the complainant. See Figure 17 in Appendix D.

86. An analysis of the complainant's spreadsheet showed many IAVs occurred only once per asset based on their unique Internet Protocol (IP) address. The spreadsheet reflects a total of 119 IAVAs, 35 IAVBs, and 92 IAVTs, which is far less than the "2,000 unmitigated IAVAs" claimed by the complainant. See Figure 18 in Appendix D.

87. In the series of e-mails sent and received by the complainant, the number of IAVs fluctuated, which demonstrated the dynamic nature of the Division's B3-COI network. Based on the 5 April 2013 e-mail sent by the complainant, several SAs responded via e-mail with explanations for the IAV findings. These explanatory e-mails are summarized below.

a. One SA explained that the "Specific CPU" (a server on the B3-COI scanned by the complainant) was under a deferral process for a remediation action ("patch") that would incorporate updated software to mitigate the vulnerability. See Figure 19 in Appendix D.

b. Another SA explained that the "Specific CPU," "Specific CPU," and "Specific CPU" (servers on the B3-COI scanned by the complainant) all had various issues that are prompting scan results to report false positives. See Figure 20 in Appendix D.

c. On 8 April 2013, a member from the IA team responded via e-mail to the complainant's initial e-mail, stating that the finding with 16 occurrences (non-IAVA) was the result of a server recently being rebuilt. See Figure 21 in Appendix D.

88. On 9 April 2013, Subject 2, RM, e-mailed the complainant an overview of the B3 remediation process. Subject 2, RM, explained:

a. "B3 scanned [sic] are conducted by AVSS [eEye Retina Scanner] once per day at 0500 and typically report in VARS by 0630."

b. "The remediation team has been tasked with managing all required patches and updates to satisfy Retina Scan findings."

c. "The compliance scans are considered only a snapshot in time as the B3 environment is highly dynamic." "It is a common occurrence to introduce 'overdue' vulnerabilities when any of these [configuration changes, STIG implementation, hardware failures, system rebuild/re-purpose] events occur."

d. "The deferral process²⁷ was placed on a very low priority during the absence of contractor staff members of the Remediation Team. Now that we have resources, we are getting all process back online." See Figure 22 in Appendix D.

89. On 9 April 2013, the complainant responded to Subject 2, RM's e-mail. The complainant addresses Subject 2, RM, as "remediation manager" and stated that he would be "happy to confer with you on the overdue assets.... unfortunately, my inquiries cannot go days at a time.... I understand there is no current Vulnerability Manager, but my assignments have taken on, in part, that role here in IA." See Figure 23 in Appendix D.

90. On 9 April 2013, the complainant e-mailed Subject 1, IAM, to discuss issues related to not being able to discuss scan results directly with the SAs. Subject 1, IAM, told the complainant that all involved would discuss, including "Witness 1, and witness 2" (contractor employees). See Figure 24 in Appendix D.

91. On 11 April 2013, the complainant e-mailed Subject 1, IAM, stating that he, along with Witness 2, and Witness 1 (contractor employees), reviewed the "scanning SOP." The complainant stated that the SOP had "all the elements you were requesting I [the complainant] put together." See Figure 25 in Appendix D.

92. On 11 and 12 April 2013, the head of the Servers and Compliance Branch, Code 114, reached out to the complainant. This occurred following the e-mail exchanges between Subject 2, RM, and the complainant. Subject 2, RM, was subordinate to the head of the Servers and Compliance Branch. The following e-mails capture the interpersonal friction between the complainant and Subject 2, RM.

a. The Servers and Compliance Branch head e-mailed the complainant asking if there was anything that could be provided to him. The complainant responded by stating: "If you prefer I address all inquiries through you prior to any lower echelon I would need to filter through my supervisor first. I am so sorry

²⁷ The deferral process occurs when an IAV cannot be immediately mitigated. It is "deferred" by submitting a Plan of Action and Milestones in OCRS that maps out the path to compliance.

this could not be resolved in a more amenable course of action but I am still hopeful this isn't the only solution." See Figure 26 in Appendix D.

b. The Servers and Compliance Branch head responded to the complainant's e-mail, and stated: "My intent was to help not make anything worse.... I noticed over the past few days there has been some tension." See Figure 27 in Appendix D.

c. The complainant responded to the Servers and Compliance Branch head's e-mail, and stated: "I understand your intent is to help communication between Subject2, RM, and myself." See Figure 28 in Appendix D.

93. On 15 April 2013, the complainant was terminated from NUWC Division Newport.

94. During the interviews conducted the week of 26-29 August 2013, the investigation team interviewed all individuals responsible for B3-COI IAV scanning, remediation, and reporting. Both the witnesses and the subjects opined that the number and types of vulnerabilities presented by the complainant in his e-mails were not surprising. However, during each respective interview, no individual stated that there was anywhere close to 2,000 IAVAs found on a daily scan. Further, no individual stated that there was ever an attempt or effort to ignore and not mitigate IAVs discovered during the daily scans. The investigation team's analysis took into consideration scans executed prior to the complainant conducting scans, and the results corroborated the witness and subject statements.

95. During the course of this investigation, SMEs from the NAVSEA Command Information Office also confirmed the validity of the statements made by the witnesses and subjects during their interviews. They stressed the fact that the daily scans are a snapshot of a dynamic network where assets were removed or introduced, and software was installed and uninstalled. IAVs discovered during one day's scans were not added to a subsequent day's scan results because each day's scan results provided the

compliance state for the network on that specific day. Further, the ability to obtain a completely clean network scan is difficult.

96. The B3-COI IAV scan results obtained by the investigation team from Subject 2 's and the complainant's computers covered the time period between 22 March 2013 and 18 April 2013. Although the B3-COI network was scanned daily, the investigation team was only able to pull nine scans from this timeframe. This timeframe was particularly important because the complainant was conducting the B3-COI IAV scans between 27 March 2013 and 15 April 2013. If the complainant did find over 2,000 IAVAs, it would have occurred during this period. The following table outlines the B3-COI scans and the corresponding number of IAVs found during each respective scan. As previously noted, the number of IAVs is not cumulative between the scans. There is a fluctuation in the quantity of IAVs because of the dynamic nature of the system. See Table 2 below.

Table 2: B3-COI Scan Results

Date of Scan	# IAVAs	# IAVBs	# IAVTs
22-Mar-13	253	19	1
27-Mar-13	101	14	1
3-Apr-13 **	30	2	1
4-Apr-13	55	22	4
5-Apr-13 **	142	2	45
8-Apr-13 **	127	44	2
9-Apr-13	55	22	4
10-Apr-13	13	0	0
18-Apr-13	232	4	0

*** Indicates a complainant conducted scan.*

Remediation Team E-mail Review

97. The e-mails obtained from Subject 2 's computer showed that ongoing business practices were employed to remediate vulnerabilities found on the B3-COI system. Additionally, these e-mails also show how the number of IAVs can fluctuate between scans. For example:

a. On 22 March 2013, Subject 2, RM, e-mailed the contractor who was responsible for remediating B3-COI vulnerabilities²⁸ a copy of the B3-COI scan results from VARS. In the attached spreadsheet, there were a total of 253 IAVAs, 19 IAVBs, and 1 IAVT. In total, there were 309 vulnerabilities found on the B3-COI network during this scan. See Figure 29 in Appendix D.

b. On 9 April 2013, Subject 2, RM, again e-mailed her contractor a copy of the B3-COI scan results from VARS and tasked her contractor to fix the vulnerabilities. In the attached spreadsheet, there were 55 IAVAs, 22 IAVBs, 4 IAVTs found on the B3-COI network during this scan. See Figure 30 in Appendix D.

Inspections Oversight

98. During 2012, U.S. Fleet Cyber Command and the NAVSEA Inspector General inspected NUWC Division Newport's IA program on two separate occasions. Although these inspections did not occur during the complainant's B3-COI scanning, they provide an unbiased historical synopsis of the Division's overall IA Program. Further, these inspections show the type of periodic outside monitoring that the Division's IA program receives. Lastly, the inspections provide insight of the Division's IAVM program.

Fleet Cyber Command Cyber Security Inspection

99. During the week of 13-17 February 2012, Fleet Cyber Command's Office of Compliance and Assessment conducted a periodic Cyber Security Inspection of NUWC Division Newport. The inspection team reviewed the following items:

a. Boundary/Network Infrastructure for the Secure Internet Protocol Router (SIPR) networks.

b. Vulnerability Scanning for the SIPR networks.

²⁸ According to witness and subject testimony, the Division was able to get support from NAVSEA for a supplemental contract. This supplemental contract was awarded during the primary IA staff contract protest. Witness 3, Witness 1, Witness 2 and Witness 4 (contractor employees) were brought back to the Division using this supplemental contract.

- c. DNS/Windows on SIPR networks, to include Gold Disk reviews.
- d. Host Based Security Systems for the SIPR networks.
- e. Traditional security items, to include policy review.
- f. Operational behavior.
- g. Program Administration.
- h. Command Directives.

100. The results of Fleet Cyber Command's Cyber Security Inspection resulted in a "satisfactory" score of 78.6%. According to Fleet Cyber Command, scores ranging between 70-89% represent a "satisfactory" score, where the level of compliance assessed reflects a satisfactory IA environment with acceptable risk to the Global Information Grid. Fleet Cyber Command's inspection team commended the NUWC Division Newport staff for the following items:

- a. Leadership engagement at all levels.
- b. Inspection seen by the command as an opportunity to excel and not as a burden.
- c. Exceptional traditional security.
- d. Solid, thorough documentation in all areas.
- e. Patching at 99.96%.
- f. 100% Information Assurance Workforce compliance.

2012 NAVSEA Inspector General Triennial Command Inspection

101. During the week of 11-15 June 2012, the NAVSEAINSGEN conducted a triennial command inspection of NUWC Division Newport. IA was one of the compliance areas reviewed by the inspection team.

102. The NAVSEAINSGEN inspection team members cited the Division's VARS as a tool that should be shared across the NAVSEA enterprise. Specifically:

"The [NUWC Division Newport] Scanning and Remediation Team developed two tools that streamline both the configuration and reporting of monthly vulnerability scans. These tools provide a centralized location the team can use to initiate and review Retina scans. The Automated Vulnerability Scanning System (AVSS) tool is used to directly initiate the Retina scanning engine without the need for human intervention. The Vulnerability Analysis and Reporting System (VARS) tool is used to parse the files generated by the Retina scanning engine into a more efficient and functional dashboard that allows the Scanning and Remediation teams to quickly ascertain the state of Information Assurance Vulnerability Management (IAVM) compliance across the different networks. It also allows them to efficiently disable systems that are in a state of non-compliance when necessary as well as re-enable them when they return to compliance.

The Inspection Team believes these tools should be made available to other NAVSEA activities for use in their vulnerability management programs."

103. For vulnerability scanning results, the compliance inspector reported:

"The Unclassified Core Infrastructure, DMZ, B3, Legacy/Residual, and Detachment scan identified two unmitigated IAVBs from 2009 and six unmitigated IAVBs from 2011. The remaining 14 IAVAs are from 2012, and have not yet reached their required compliance date. Overall 18 distinct IAVs were found."

104. Overall, the IA portion of the NAVSEAINSGEN Inspection received a "Satisfactory" rating.

105. As of 3 October 2012, the IA corrective actions were closed out in the NAVSEAINSGEN Inspection Plan of Action and Milestones tracking database. The command compliance lead stated:

"All findings have been cleared or documented as backport²⁹ issues. OQE [Objective Qualifying Evidence] provided with DISA [Defense Information Systems Agency] Ticket numbers for backports and false positive Retina findings³⁰."

106. On 1 August 2013, the IA compliance inspector from NAVSEA's Command Information Office e-mailed the investigator and stated:

"As you can see from the inspection report and cards, the IAVM program was good at the time of the inspection. We didn't find a whole lot of open vulnerabilities but some were from back as far as 2009 and some of them were significant. Overall, we have seen worse programs."

Discussion and Analysis

107. The complainant's claim that "2,000 unmitigated IAVAs" existed on NUWC Division Newport's networks is unfounded. Further, there were no separate "high-risk" IAVAs, as all IAVAs are considered the highest risk.

108. While NUWC Division Newport's domains did contain IAVs, an analysis of multiple scan results confirmed that NUWC Division Newport actively addressed IAVs found during its daily scans. These scan results encompassed the timeframe that the

²⁹ Backporting is the action of taking a certain software modification (patch) and applying it to an older version of the software. Backports, although remediating an IAV, can still show up on a Retina Scan.

³⁰ False positive Retina findings are vulnerabilities that show up on a Retina Scan, but do not actually exist on the network. The Defense Information Systems Agency (DISA) assigns a helpdesk ticket when a Retina scan issues a false positive, i.e. an asset that was patched but continues to show as a vulnerability. DISA amends the scanning tool code to correct the scan results in the future.

complainant was assigned to scan NUWC Division Newport's B3-COI networks for IAVs. There was no conflicting testimony between the witnesses and the subjects concerning the number of IAVs found on the Division's B3-COI network. All testimonies independently verified that the number of IAVAs alleged by the complainant to have existed on the Division's B3-COI network was unfounded. The business practices analyzed by the investigation team showed ongoing efforts by the Division's personnel to remediate IAVs discovered during IAV scans.

109. CTO 11-16 requires Navy activities to scan and remediate computer networks at a minimum of every 30 days. SECNAV M-5239.1 has assigned the IAM as the primary individual responsible for IAVM. NUWC Division Newport has also designated the Remediation Manager as a member of the IAVM process to ensure remediation actions are taken for centrally managed networks. Subject 1's, IAM, responsibility, as the IAM for NUWC Division Newport, was to ensure the Division's networks were scanned and IA vulnerabilities addressed. Supporting Subject 1 in her role as IAM, Subject 2, RM, supported the remediation of servers in her role as the Remediation Manager.

110. NUWC Division Newport improved upon CTO 11-16 requirements for monthly IAV scans by conducting scans on a daily basis. Scan results were then displayed using an internally developed software solution called VARS. VARS provided enhanced visibility of IAVs on the Division's networks by all IA personnel. This almost real-time network scanning greatly reduced the command's IA risk when compared to the monthly network scan and mitigation requirements.

111. The investigation team was unable to find anywhere close to "2,000 unmitigated IAVAs" during its analysis of nine scans conducted by the division from 22 March 2013 to 18 April 2013. As stated previously, the complainant was conducting B3-COI IAV scans during this timeframe. The complainant would have seen and communicated the number of IAVAs found during this timeframe. Further, there was no mention of "over 300 high-risk vulnerabilities" by the complainant. The below table outlines the B3-COI scans and the corresponding number of IAVs found during the complainant's B3-COI scanning tenure. See Table 3.

Table 3: B3-COI Scan Results

Date of Scan	# IAVAs	# IAVBs	# IAVTs
22-Mar-13	253	19	1
27-Mar-13	101	14	1
3-Apr-13 **	30	2	1
4-Apr-13	55	22	4
5-Apr-13 **	142	2	45
8-Apr-13 **	127	44	2
9-Apr-13	55	22	4
10-Apr-13	13	0	0
18-Apr-13	232	4	0

*** Indicates a complainant conducted scan.*

112. As stated previously in this report, the number of IAVs discovered during each scan was not cumulative. Each scan result represented the state of IAVs on the network for that given time. The fluctuating number of IAVs identified in the VARS system during the March-April 2013 timeframe highlighted the dynamic nature of the B3-COI network. The fluctuating number of IAVs found during the daily scans highlighted the Division's ongoing efforts to remediate vulnerabilities based on those scan results.

113. During interviews of the subjects, witnesses, and SMEs, all independently stated that NUWC Division Newport's daily scans never approached 2,000 IAVAs. During the e-mail reviews of the subject and complainant's computers, there was never a mention of an exceedingly high figure of IAVAs. These e-mail reviews of the subjects' computers corroborated efforts to address IAVs found via scanning. Lastly, none of the nine scan analyzed by the investigation team contained close to 2,000 IAVAs.

114. A review of business practices and inspection results provided an unbiased look at how the Division actively addressed IAVs. The Division received two "satisfactory" inspection results of its IA program in 2012. The proactive efforts undertaken by NUWC Division Newport to address IA vulnerabilities were praised during these inspections as a best practice amongst Navy activities. Additionally, the evidence showed that the remediation manager was actively addressing IAVs found during scans of the B3-COI system.

115. With any computer network, there is a risk that disreputable individuals could exploit unmitigated IA vulnerabilities. These IA vulnerabilities can, and do, appear daily as software and IT assets change. NUWC Division Newport has taken steps to reduce its risk by developing VARS to maintain an almost real-time visibility on network vulnerabilities. Compared to NCDOC's monthly scanning requirement, the Division's daily scanning of the B3-COI system allows the command to have an up-to-date view of the vulnerabilities affecting the domain. These vulnerabilities are shared with the respective IA personnel for remediation action. This system of daily scans and remediation does not remove the risk of access and manipulation of "hundreds of IT devices" but it does reduce this risk.

116. In reaching this conclusion, the investigation team did not discount the fact that there were, and will continue to be, IAVs on NUWC Division Newport's networks. The dynamic nature of IT systems, where manipulation of software and hardware occurs on a continual basis, will always prompt new vulnerabilities to appear, or previously mitigated vulnerabilities to reappear.

117. In summary, the investigation team reviewed all relevant scans for the timeframe in which the complainant was conducting B3-COI IAV scans and the team could not find 2,000 unmitigated IAVAs. The investigation team interviewed all personnel who would have seen the B3-COI scan results, and no one provided testimony that supported the complainant's allegations. Based on scan results, interviews, SME testimony, and NUWC Division Newport's past business practices, we concluded that the allegations were not correct and the activity took appropriate action on each IAVA that was discovered. Subject 1, IAM, carried out her duties as the IAM pursuant to SECNAV M-5239.1, section 2.4.9. for the mitigation of IAVs. Subject 2, RM, carried out her duties as the Remediation Manager pursuant to NUWC Division Newport Vulnerability Management Plan.

Conclusion

118. The allegation that Subject 1, IAM, Naval Undersea Warfare Center Division Newport, Newport, Rhode Island, between March and April 2013, failed to mitigate known information assurance vulnerabilities, in violation of SECNAV M-5239.1, section 2.4.9. is not substantiated.

119. The allegation that Subject 2, RM, Naval Undersea Warfare Center Division Newport, Newport, Rhode Island, between March and April 2013, failed to mitigate known information assurance vulnerabilities, in violation of NUWC Division Newport Vulnerability Management Plan is not substantiated.

Observations and Recommendations

120. Between the complainant's initial assignment to conduct B3-COI scanning, and the subsequent meeting to discuss the Division's scanning and remediation process, the complainant's training on the Division's processes appeared to be experiential³¹. The fact that the complainant reported that there were "over 2,000 unmitigated IAVAs, 300 of which were high-risk vulnerabilities," when the scans captured less than 300 IAVAs at any one time, showed a lack of understanding of the IAVM process, the hierarchy of IA vulnerabilities, and the overall B3-COI system. The complainant's representation of IAVAs, followed by statements that there were additional "high-risk vulnerabilities," indicate a lack of understanding of IAVs.

121. Because VARS was a locally-developed system, the complainant should have received training on the operation of the system as well as the underlying policies and procedures. Discussions about SOP development and review occurred after the complainant conducted scans and reported to the IA workforce. A thorough understanding of both the system and the process could have reduced the friction between the complainant and other Division employees regarding scan results and remediation efforts.

³¹ Experiential learning is the process of making meaning from direct experience, i.e., learning from experience rather than acquiring information through the study of a subject.

122. The lack of a vulnerability manager, and the reliance on contractors to conduct scanning operations, contributed to the complainant's misunderstanding of the system and processes for IA scanning and remediation. According to testimony from witnesses and subjects, the vulnerability manager position has remained vacant since mid-2012. As a result, Subject 1 and the contracted support staff in Code 1153 absorbed the duties of the vulnerability manager. The complainant's involvement in B3-COI scanning was on an experiential basis. There was no vulnerability manager to facilitate information sharing about the process. This could have led to confusion about NUWC Division Newport scanning and remediation processes. Only after a series of e-mail exchanges did the complainant, the IAM, and the two Code 1153 IA contractors collectively sit down and discuss the scanning and remediation processes. This discussion occurred one week following the complainant's initial B3-COI scan results e-mail.

123. The inability to maintain IA scanning and remediation continuity of operations is a risk to the security of the GIG. Investigation team observations and the subjects' own admissions revealed that NUWC Division Newport placed a heavy reliance on contractors to support the IA scanning and remediation programs. The result of this reliance, coupled with the contract protest, posed a considerable risk on IA program execution.

124. During Subject 1's, IAM, interview, she stated that she was putting together hiring packages in an attempt to convert contracted staff to government positions. However, due to the "hiring freeze," plans to fill vacant IA positions have been delayed. At a minimum, the conversion of these contracted positions should be a priority given the circumstances that affected the NUWC Division Newport IA and IT branches.

Allegation Three

That Subject 1, IAM, Naval Undersea Warfare Center Division Newport, Newport, Rhode Island, between March and April 2013, falsely reported information assurance vulnerabilities as being "Fully Compliant," in violation of SECNAV M-5239.1, section 2.4.9. (Not substantiated).

What the Complainant Contends

125. The 3 July 2013 OSC tasking letter states that the subjects misreported IAVAs as "Fully Compliant" to DoD via OCRS. Specifically, the complainant stated, "at least eleven high-risk IAVAs were misreported" and that the unmitigated IAVs pose a threat to the entire NUWC Division Newport network.

126. Within the OSC tasking letter, the complainant alleged that by reporting "Fully Compliant" in OCRS, NUWC Division Newport would save itself from embarrassment when NCDOC sends out non-compliance Navy messages.

127. During the complainant's interview on 1 August 2013, he stated that the contracted support was responsible for reporting IAV compliance in OCRS. He alleged that the contractors would report compliance in OCRS, regardless of actions taken. The complainant also questioned the ability to manipulate data within OCRS following initial entry, stating that he was concerned that records could have been destroyed in light of his termination and subsequent complaint³².

128. On 4 August 2013, the complainant provided a copy of specific IAVAs that he believed were misreported as being "fully compliant." In this list, the complainant identified 14 (11 were mentioned in the OSC tasking letter) IAVs he believed were misreported as being "fully compliant." The complainant did not provide an explanation of why his list contained more IAVAs than

³² The complainant made this passing remark to the investigation team during his initial interview. The complainant stated that he was concerned that Division personnel may manipulate data based on this complaint. He provided no evidence to validate this claim.

what was in the initial OSC complaint. See Figure 31 in Appendix D.

129. The complainant's list (Figure 31 in Appendix D) annotated fourteen different IT assets, each with a unique IP address, that were purported to have unmitigated IAVs. Using an asterisk, the complainant indicated the machines that he believed to have IAVs that were "falsely reported" in OCRS. The complainant's table was generated from the Division's VARS system. The complainant told the investigation team that he had generated this printout prior to his termination from NUWC Division Newport.

130. The investigation team analyzed the complainant's list of IAVs; by comparing that list to prior scan results; comparing the complainant's IAV list to the OCRS reporting; and leveraging SMEs to provide analysis of the network scan results and corresponding OCRS reporting.

Complainant's Initial IAV and OCRS Reporting Concerns

131. On 4 April 2013, the complainant sent an e-mail to Subject 1, IAM, discussing issues about scan results and the reporting in OCRS. This e-mail was also the beginning event concerning the facts discussed in Allegations One and Two. See Figure 32 in Appendix D.

132. On 8 April 2013, the complainant sent an e-mail to Subject 1, questioning an IAVA that was marked as "fully compliant" in OCRS but still appeared in the VARS system as deficient. See Figure 33 in Appendix D.

Findings

133. The following facts are pertinent to the allegation made by the complainant that "at least eleven high-risk IAVAs" were being misreported as "fully complaint" in the OCRS.

134. This section addresses the general facts pertinent to this allegation, the NUWC Division Newport OCRS reporting process, the investigation team's analysis of OCRS and VARS scan results, and retroactive compliance reporting.

General Facts

135. The Division's "Vulnerability Management Plan" outlined the compliance reporting requirements for the Division. To determine the accuracy of compliance reporting, the investigation team reviewed the OCRS reporting process, interviewed those responsible for OCRS reporting, and reconciled scan results conducted during the complainant's tenure against the compliance reporting done in OCRS.

136. As reported in earlier sections of this report, e-mails obtained from the subjects' and complainant's government computers contained scan results for the timeframe that the complainant was conducting IAV scans of the B3-COI network. These historical scan results allowed the investigation team to search for the IAVs alleged by the complainant to have been falsely reported by the Division. While analyzing the scan results, the investigation team obtained access to the OCRS system to get an unbiased look at the Division's IAV compliance reporting. This review of OCRS included both historical reporting and current reporting done by the Division. The investigation team reconciled scan results to the OCRS reporting in order to determine if OCRS reporting accurately reflected the Division's IAV scans for the B3-COI network. Lastly, an SME from the NAVSEA Command Information Office provided an additional review of the VARS scan results, the OCRS compliance reporting, and the corresponding mitigation procedures in place.

137. There were two internal control mechanisms in place to ensure accurate reporting in OCRS by NUWC Division Newport personnel. The first control mechanism was a separation in duties. As discussed earlier in the report, Code 1153 conducted the IAV scans and reported compliance in OCRS, while Code 1142 remediated the vulnerabilities. The second internal control was the separation in systems. Data in the OCRS system, which tracked IAV compliance and mitigation plans, was manually entered by Code 1153 personnel based on VARS scan results. VARS scan results captured the efforts of Code 1142's remediation efforts. Because Code 1153 personnel entered OCRS compliance information manually, a misreported remediation action in OCRS would continue to appear in subsequent scans in VARS and undergo

remediation by Code 1142. These controls ensured that the Division was addressing IAVs, and that those actions corresponded to what was reported in OCRS.

138. While the three Code 1153 contractor personnel (Witness 1, Witness 2, and Witness 4) indicated that they were the only individuals who had the day-to-day responsibility of reporting IAV compliance, each separately denied falsely reporting IAV compliance in OCRS during their respective interviews. Further, they each separately stated that neither Subject 1, IAM, nor any other individual ever instructed them to misreport IAV compliance in OCRS.

139. The investigation team was unable to find any e-mail evidence that identified the 11 or 14 falsely reported IAVAs raised by the complainant during his tenure at NUWC Division Newport. The complainant provided the list of IAVs (Figure 31, Appendix D) to the investigation team during the course of their investigation.

140. Many of the findings of fact pertinent to this allegation also appear in the findings section for Allegations One and Two.

NUWC Division Newport OCRS Reporting Process

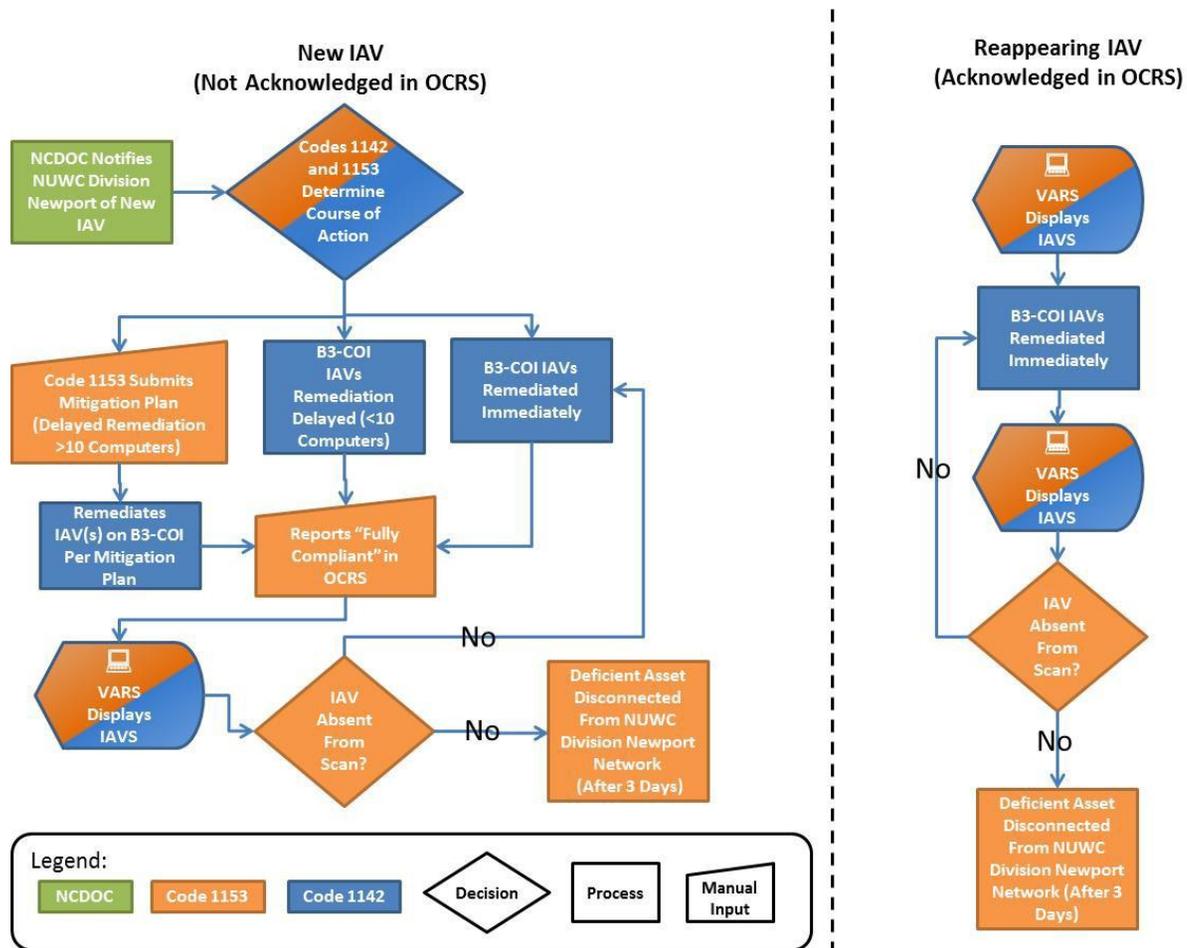
141. During the interviews conducted by the investigation team, witnesses and subjects were questioned about the process to report compliance. The three (contractor employee) witnesses (Witness 1, Witness 2, and Witness 4), along with Subject 1, IAM, indicated they were the only individuals responsible to report compliance in OCRS. The access roster in OCRS confirmed that these four individuals were the only ones with access to the database (see Figure 34 in Appendix D) although NAVSEA's Command Information Office and NCDOC also have visibility into OCRS. As of the time of this report, Subject 2, RM, did not have access to OCRS.

142. Witness 4 (contractor employee) told the investigators that she is the individual responsible for acknowledging and reporting the disposition of IAVs within OCRS. During her interview, Witness 4 stated that she would report IAV compliance based on patch or mitigation deployment. She

explained that either (1) a patch would be successfully installed and not show up in subsequent VARS scans, or (2) the IAV would show up on subsequent VARS scans and the machine would be disconnected within three days based on the Division's established procedures. A machine that was disconnected from the network would not appear on subsequent scans.

143. Code 1153 and Code 1142 personnel followed prescribed procedures to report compliance in OCRS based on VARS scan results. When a new IAV was introduced by NCDOC, the remediation action would be subject to OCRS reporting. New IAVs would be subjected to one of three possible scenarios: (1) immediate remediation where patches would be installed and compliance would be reported; (2) delayed remediation (patches would be pushed to the computers but installation would be delayed due to a delayed restart) and compliance would be reported; or, (3) if the IAV could not be remediated in the time specified by NCDOC, Code 1153 personnel would request a mitigation plan to extend the IAV's compliance deadline. Regardless of the scenario, Code 1153 personnel would report the Division's efforts into OCRS based on the VARS scan results. Figure 4 on the following page outlines the NUWC Division Newport process to report IAV compliance in OCRS.

Figure 4: NUWC Division Newport OCRS Reporting Process



144. All witness interviews independently confirmed that compliance reporting in OCRS is coordinated internally. They report the number of assets affected and remediated based on the scan results contained in VARS. If they felt that the IAV could not be remediated in the prescribed timeframe, Witness 4 would submit a mitigation plan in the OCRS system. No witness stated that they, or any of their coworkers, were instructed to misreport IAV compliance in OCRS.

145. The three witnesses in Code 1153 (Witness 1, Witness 2, and Witness 4, all contractor employees) all separately stated that once a patch was deployed to remediate an IAV, there was a chance that the patch install could be delayed. For example, a delay could occur in situations where a server could not be restarted until a future date due to Division requirements³³. In situations like this, Witness 4 reported an IAV as being "fully compliant." The witnesses all separately stated that this situation happened only when a few machines (generally less than 10) were affected. Following the restart, if the patch install was unsuccessful, VARS scan results would continue to show the IAV. If further remediation was not successful, the asset was disconnected from the system in accordance with NUWC Division Newport policies.

146. The three witnesses in Code 1153 all stated that if there were more than 10 machines that could not be patched prior to the IAV compliance date, Witness 4 would submit a mitigation plan in OCRS. NCDOD would review the mitigation plan, and outline the path to compliance (outlining the number of assets to be remediated using a plan of actions and milestones). The Division was required to report on the ongoing remediation efforts in OCRS. Once the Division fulfilled the mitigation plan requirements, it would report compliance in OCRS. To ensure personnel were actively working to meet the mitigation plan requirements, VARS would continue to show the IAVs, but would list the IAVs as deferred. The compliance dates in VARS would also be adjusted to reflect the mitigation plan dates. This ensured that an IAV was not overlooked while a remediation

³³ The asset is turned off and restarted during the loading of a patch. Based on requirements imposed by NUWC Division Newport staff, there is a chance that the machine restart could be delayed due to Division requirements.

action was delayed. If the IAV was not mitigated by the revised compliance date per the mitigation plan, Code 1153 would disconnect the asset.

147. These standing policies had been in place prior to the complainant's tenure. For example, on 22 January 2013, Subject 1, IAM, provided amplifying guidance to the Vulnerability Management Plan and Remediation SOP guidance via e-mail. Specifically, the message captured the three-day timeline in relation to non-IAV compliance and subsequent disconnection from the network. See Figure 35 in Appendix D.

148. The three witnesses (contractor employees) in Code 1153 all separately stated that OCRS reporting is based on VARS scan results. If a particular IAV was unsuccessfully mitigated following a remediation action, it would continue to appear on subsequent scan results. If the IAV remains, after three days, the deficient asset would be disconnected from the network in accordance with the Division's Vulnerability Management Plan and Remediation Process SOP. Subject 1, IAM, and Witness 4 also confirmed these statements during their respective interviews.

149. The investigation team questioned the subjects and witnesses as to what would happen if an IAV was not mitigated, but was reported in OCRS as being "fully complaint." Separately, the witnesses and subjects all stated that scan results would continue to show the unmitigated IAV in subsequent scans. OCRS and VARS were separate systems, where OCRS required manual entry of IAV information based on the VARS scan results. Any IAV that was reported as "fully complaint" in OCRS would only be on the network for three days before it was remotely disconnected by Code 1153. One contractor called the practice of three-day disconnection "cut throat," because system administrators are not notified about the system disconnect before it occurs. The process of disconnecting the system from the network reduced the risk of the non-complaint IAVs being exploited while they are in the process of being fixed.

150. During interviews and e-mail reviews, the investigation team found no evidence to indicate that either Code 1153 or 1142 undertook efforts to circumvent the Division's IAVM program controls discussed previously.

NUWC Division Personnel Response to the Complainant

151. On 8 April 2013, Subject 1, IAM, responded to the complainant via e-mail about the issues with scan results re-appearing after a remediation. Specifically, the complainant questioned one IAVA that was found on two assets. Subject 1, IAM, directed the complainant to discuss these issues with IA contractor [Witness 1]. See Figure 36 in Appendix D.

152. On 8 April 2013, Witness 1 (contractor employee) responded via e-mail to the complainant's initial e-mail about IAVs being reported as "fully compliant." Witness 1 stated that the reason for the reappearance of a previously mitigated vulnerability was due in part to "two computers being patched but both computers [were] waiting for a reboot, and have not yet hit their designated reboot time." See Figure 37 in Appendix D.

Investigation Team's Analysis of Alleged Misreported IAVs

153. Following the complainant's interview on 1 August 2013, the investigation team was provided a list of IAVs. See Figure 31 in Appendix D. The list provided by the complainant was prepared using VARS. The complainant identified fourteen individual IT assets (each with a distinct IP address in the "IP" column) that were purported to have unmitigated IAVs that were falsely reported in ORCS. Each alleged noncompliant machine was marked with an asterisk by the complainant (seen next to the "AuditID" column). The "first seen" column indicates the time the VARS daily scan first picked up the IAV on that specific asset. The "last seen" column indicates when the IAV was last seen on a daily scan for a specific asset. Although the complainant did not indicate when the printout was created, the investigation team assumed that the printout was created on 3 April 2013 given that all the "Last Seen" dates occurred on 3 April 2013.

154. In order to determine if the identified IAVs provided by the complainant were unmitigated and incorrectly reported as "fully compliant" in OCRS, the investigation team first compared Code 1153's OCRS entries to the complainant's VARS printout. Any IAVs with different "first seen" and "last seen" dates could have been unmitigated, thereby making the OCRS reporting inaccurate. Next, the investigation team reviewed the nine extant VARS scan results to determine if those fourteen IAVs went unmitigated. Any unmitigated IAVs found on each day's scan results, yet identified as "fully compliant" in OCRS reporting, would be inculpatory to the complainant's allegation of false reporting in OCRS. However, if an IAV appeared in a scan result but disappeared in a subsequent scan, it would be an indication that NUWC Division Personnel had taken action to properly address the IAV (either by disconnecting the asset or remediating the IAV).

155. The investigation team's analysis found that all IAVs identified by the complainant were identified as "fully compliant" by Code 1153 in OCRS. OCRS captured the IAV's compliance state at a specific point in time, in this case, the "Report Last Modified"³⁴ date. The investigation team compared the "Report Last Modified" OCRS date to when the IAVs were "first seen" and "last seen" on the complainant's scan results.

156. On the next page, a table is presented for the ease of comparing dates.

³⁴ The complainant provided us Figure 31. The "Report Last Modified" date addressed any concerns about OCRS information manipulation following the complaint to OSC.

Table 4: Complainant-Provided IAV List and OCRS Status

IP (VARS)	IAV Number (VARS)	Status (OCRS)	Report Last Modified (OCRS)	First Seen (VARS - Date Only)	Last Seen (VARS-Date Only)
Specific CPU #	2013-A-0031	Fully Compliant	2/11/2013	2/27/2013	4/3/2013
Specific CPU #	2013-A-0031	Fully Compliant	2/11/2013	2/27/2013	4/3/2013
Specific CPU #	2013-A-0031	Fully Compliant	2/11/2013	2/27/2013	4/3/2013
Specific CPU #	2013-A-0031	Fully Compliant	2/11/2013	2/27/2013	4/3/2013
Specific CPU #	2013-A-0057	Fully Compliant	3/25/2013	4/3/2013	4/3/2013
Specific CPU #	2013-A-0031	Fully Compliant	2/11/2013	2/27/2013	4/3/2013
Specific CPU #	2013-A-0031	Fully Compliant	2/11/2013	2/27/2013	4/3/2013
Specific CPU #	2013-A-0031	Fully Compliant	2/11/2013	2/27/2013	4/3/2013
Specific CPU #	2013-A-0004	Fully Compliant	1/21/2013	1/15/2013	4/3/2013
Specific CPU #	2013-A-0004	Fully Compliant	1/21/2013	1/15/2013	4/3/2013
Specific CPU #	2013-A-0004	Fully Compliant	1/21/2013	1/15/2013	4/3/2013
Specific CPU #	2013-B-0001	Fully Compliant	2/19/2013	4/3/2013	4/3/2013
Specific CPU #	2013-A-0006	Fully Compliant	1/21/2013	4/3/2013	4/3/2013
Specific CPU #	2013-A-0057	Fully Compliant	3/25/2013	4/3/2013	4/3/2013

Note: Red shading indicates an IAV that appeared on the VARS scan prior to when the Division reported "Fully Compliant" in OCRS. Blue shading indicates that an IAV was "first seen" and "last seen" by the VARS scan on the same date.

157. The complainant's list of IAVs provided enough information to determine if an (falsely reported) IAV was present in any of the nine scan results. Using Microsoft Excel's "countif" function, the complainant's list of IAVs was compared to the nine VARS scan results obtained from the complainant's and subjects' computers. The Excel function searched for the specific asset IP address, eEye Retina Audit ID, and the (falsely reported) IAV identified by the compliant. If an asset's specific IP address did appear with the corresponding IAV, a "yes" would appear. See Figure 5 below.

Figure 5: Investigation Team's Analysis of IAVA Scan Results

Complainant Provided IAVA/B Listing			VARS Scan Results								
IP	IAVA/B	Audit ID	22-Mar-13	27-Mar-13	3-Apr-13	4-Apr-13	5-Apr-13	8-Apr-13	9-Apr-13	10-Apr-13	18-Apr-13
Specific CPU #	2013-A-0031	18127	Yes	--	--	--	--	--	--	--	--
Specific CPU #	2013-A-0031	18127	Yes	--	--	--	--	--	--	--	--
Specific CPU #	2013-A-0031	18127	Yes	--	--	--	--	--	--	--	--
Specific CPU #	2013-A-0031	18127	Yes	--	--	--	--	--	--	--	--
Specific CPU #	2013-A-0057	19369	--	--	--	--	--	--	--	--	--
Specific CPU #	2013-A-0057	18370	--	--	Yes	--	--	--	--	--	--
Specific CPU #	2013-A-0031	18127	Yes	--	--	--	--	--	--	--	--
Specific CPU #	2013-A-0031	18127	Yes	--	--	--	--	--	--	--	--
Specific CPU #	2013-A-0004	17941	Yes	--	--	--	Yes	--	--	--	--
Specific CPU #	2013-A-0004	17941	Yes	--	--	--	Yes	--	--	--	--
Specific CPU #	2013-A-0004	17941	Yes	--	--	--	Yes	--	--	--	--
Specific CPU #	2013-B-0001	17947	--	--	--	--	--	--	--	--	--
Specific CPU #	2013-A-0006	17865	--	--	--	--	--	--	--	--	--
Specific CPU #	2013-A-0057	18370	Yes	--	Yes	--	--	--	--	--	--

158. The above analysis reconciled the complainant's list of IAVs falsely reported as "fully compliant" after remediation, against the scan results obtained during the course of this investigation. Instances where a particular IAV appeared during one day's scan were promptly addressed, as it did not reappear in subsequent scans. During interviews, the witnesses responsible for conducting daily IAV scans stated that a particular IAV could reappear as an asset's configuration (hardware and software) changed. Witnesses pointed out that when an IAV did not show up on a subsequent scan, there was conclusive evidence that it was addressed by a remediation action. Nevertheless, an IAV addressed through remediation, and reported as compliant in OCRS as "fully compliant," may still

have been identified in a subsequent scan. As explained in paragraph 145, a remediation action did not always take effect immediately.

159. During the week of 26-29 August 2013, a representative from NAVSEA's Command Information Office reviewed the VARS reporting and compared it to mitigation plans, Defense Information Systems Agency (DISA) ticket numbers, and OCRS compliance reporting. Four networks were selected randomly for review: a research and development lab, a stand-alone network, a small lab, and the B3-COI. All scan results reviewed were on the unclassified networks.

160. Based on the SME review, it appeared that NUWC Newport's IAV program was being operated properly. For those IAVs that existed on the Division's networks during the SME's review that were in a state of non-compliance, the SME found either an approved deferral (mitigation plan) in place or a corresponding DISA helpdesk ticket number associated with the VARS scan result.

Retroactive Compliance Reporting in OCRS

161. During the course of this investigation, the requirements for amending a "fully compliant" OCRS report for an IAV that reappeared on the network were unclear. During the witness and subject interviews, no one stated that they would go back into OCRS to change a "fully compliant" IAV status based on a previously reported IAV reappearing on the network. Rather, they would just address the IAV through a remediation action. Throughout all interviews conducted at NUWC Division Newport, it was apparent that Code 1153 reported on IAVs within upcoming OCRS compliance dates.

162. On 28 August 2013, the NCDOC SME provided an explanation to the investigation team outlining compliance reporting requirements for previous "fully compliant" IAVs. See Figure 38 in Appendix D.

163. The NCDOC SME directed the investigation team to NCDOC Directive 11-001, dated 07 December 2011. Directive 11-001 provided updated guidance on scanning and remediation procedures for all Navy assets. Part two specifically states:

"2. (U/FOUO) ALL NAVY COMMANDS ARE TO CONDUCT SYSTEM SCANS AT LEAST ONCE A MONTH PER REF A [JTF-GNO CTO 08-001].... ALL MONTHLY SCANS ARE TO BE MAINTAINED FOR A MINIMUM OF 90 DAYS, TO INCLUDE DEPLOYED UNITS, AND WILL BE PROVIDED TO NCDOC WHEN DIRECTED."

164. Specifically, the NCDOC SME stated:

If I scan on 01 July and there are no findings then that is what I report in OCRS. Something may happen the very next day to put me out of compliance and if I'm aware of this the expectation is that I scan, remediate, and rescan to see if the problem is corrected (para 3 and the establishment of a vulnerability management program). If the issue remains undetected until I scan again on 01 August then I have done nothing wrong but I am supposed to properly report the new findings.

Discussion and Analysis

165. Evidence collected during this investigation did not substantiate the allegation that IAVs provided by the complainant were misreported in the OCRS system or went unmitigated. Consequently, the team also found no evidence to support the complainant's concern that IAVs went unmitigated and posed a risk of manipulation to NUWC Division Newport's networks. There was no evidence that would indicate that the reporting in OCRS was inaccurate. The investigation team concluded that IAVs identified by the complainant, which reappeared following the compliance reporting in OCRS, were due to asset configuration changes on the Division's dynamic network.

166. The investigation team analyzed internal controls for the scanning and reporting of IAVs in OCRS. Nine separate B3-COI network scans were reconciled against OCRS to determine if NUWC Division Newport IA staff accurately reported and addressed IAVs identified by the complainant. The three individuals responsible for reporting in OCRS stated that they never falsely reported IAV compliance nor were they instructed to falsely report compliance. NUWC Division Newport personnel did discuss legitimate reporting practices that might still result in a remediated IAV showing as "fully compliant" in subsequent scans. The investigation team identified no evidence to support a conclusion that any information provided by NUWC Division Newport into OCRS was anything other than as accurate as possible.

167. SECNAV M-5239.1 assigned the IAM as the primary individual responsible for IAVM. In the case of NUWC Division Newport, Subject 1, IAM, was the individual responsible for IAVM. According to the NUWC Division Newport Vulnerability Management Plan, the Remediation Manager, Subject 2, had no assigned responsibility for OCRS compliance reporting. As a result, the sole responsibility for accurate OCRS reporting fell upon Subject 1, IAM.

168. The investigation team reviewed the Division's OCRS reporting process and found that there were adequate controls in place to support accurate reporting. The Division's controls were set up in such a way that no single Code retained all the required duties to execute the Division's IAVM program. For deliberate misreporting in OCRS and the non-mitigation of IAVs to have occurred, Code 1153 and Code 1142 would have had to collectively circumvent the controls in place. For example, if Subject 1, IAM, and Code 1153 staff falsified compliance reporting in OCRS, VARS scan results would have still showed IAVs. Code 1142 would then have had to manipulate the VARS scan results to indicate a remediation action had taken place. However, the time-stamps of e-mails, dates of the scan results, and OCRS "last reported" dates analyzed by the investigation team found no evidence of manipulation following the complainant's termination. Further, the investigation team found no evidence in the e-mails reviewed or during interviews

to indicate that there was collusive behavior between the two office codes to misreport IAVs in OCRS. As a result, the investigation team found reasonable assurance that the two Codes adhered to standing policies to ensure that IAVs were addressed, accurate OCRS reporting was conducted, and that the risk to the Division's network was reduced.

169. The non-compatibility of VARS and OCRS provided a control mechanism to ensure Code 1153 and Code 1142 personnel were executing their assigned responsibilities. The two systems did not automatically transfer information, which required manual inputs by Code 1153 and Code 1142 personnel. This involvement meant that the two Codes could maintain awareness over the other Code's ongoing efforts. For example, the mutual exclusivity of the systems meant that even with a "fully compliant" OCRS status, any IAV that remained on the network would remain visible based on scan results. As a result, the IAV would be addressed by either Code 1142 (remediated) or Code 1153 (remotely disconnected) based on the daily VARS scan results.

170. Based on the investigation team's review of complainant's list of IAVs and the nine scan results, there was reasonable assurance that Division personnel were actively addressing IAVs (identified by the complainant). Any attempt to not remediate the identified IAVs identified by the complainant would have shown in all nine scans. However, the IAVs identified by the complainant were not found during subsequent scans. This provided additional assurance to the investigation team that information captured in OCRS was as accurate as possible.

171. Within a properly running IAVM program, there is a potential that IAVs reported as "Fully Compliant" in OCRS may reappear. However, this is due to the dynamic nature of the system. Given the fact that OCRS only provides a static view for IAV compliance, the daily scanning and configuration changes to the NUWC Division Newport networks meant OCRS and VARS results might not have always reconciled. Evidence obtained through interviews and e-mail reviews showed an engaged effort by Code 1153 and 1143 personnel to address IAVs that reappeared within VARS.

172. The reappearance of an IAV in later scans is not inconsistent with proper procedures and a proper response to IAVs. If an IAV did continue to go unmitigated, the asset would be disconnected from the network after a period of three days. The evidence clearly showed that the Division's IA personnel were actively addressing the IAVs, as they did not reappear on subsequent scans. This gave reasonable assurance that the information reported into OCRS was accurate, and the corresponding risk to DoD networks was reduced.

173. NUWC Division Newport's policy of reporting IAV compliance in OCRS based on patch deployment, vice successful install, may have contributed to the complainant's concerns. Based on IT demands, not all assets could be rebooted immediately following updates or patch deployments. If the number of affected assets were minimal, compliance would be reported in OCRS. However, if there were numerous affected assets, the team submitted a mitigation plan. For those IAVs that were reported compliant while awaiting implementation, IA staff members were still able to maintain awareness using the VARS system. If an IAV was still present for a particular asset after three days, the asset would be disconnected from the network per the Division's Vulnerability Management Plan.

174. DoD and DON policies concerning retroactive compliance reporting in OCRS were unclear and could have contributed to the misunderstanding of IAV OCRS reporting. Witness and subject interviews illustrated that only IAVs with upcoming due dates were addressed in OCRS. There was no effort to go in and change the status of previous reported IAVs. Division personnel only took action to remediate a previously reported IAV found in VARS. In discussions with the NCDOC SME, guidance stated that compliance must be reported monthly if scan results show non-compliance. With daily scan results and remediation actions taking place at NUWC Division Newport, any additional requirements to update OCRS would be onerous.

175. Overall, the processes to report IAV compliance into OCRS based on scan results, coupled with the proactive remediation efforts by the NUWC Division Newport Staff and visibility by

senior commands into data in OCRS, ensured accurate reporting. The Division conducted daily network scans and addressed IAVS through remediation actions or mitigation plans. The Division had the requisite policies and procedures in place to reduce the risk to NUWC Division Newport's domains. The actions undertaken by Subject 1, IAM, and Subject 2, RM, to address IAVS reduced the risk to NUWC Division Newport's IT assets, and its connected networks.

176. In summary, the investigation team reviewed the OCRS reporting process at NUWC Division Newport, reviewed the IAVs alleged by the complainant to have been falsely reported in OCRS as being "fully compliant" without being fixed, and interviewed relevant individuals that were involved with OCRS reporting. Based on the investigation team's analysis, there were controls in place to ensure that the Division remediated IAVs and accurately reported compliance in OCRS. The analysis done by the investigation team found no evidence to indicate that IAVs went unmitigated while reported as being "fully compliant" in OCRS. B3-COI scan results showed that IAVs were actively addressed, because they did not reappear on subsequent scans. Interviewed Division personnel stated that they did not falsely report IAV compliance in OCRS, and that they were not instructed to make false reports in OCRS. SMEs also opined that NUWC Division Newport personnel addressed IAVs and reported accurate information into OCRS. As a result, this investigation concluded that Subject 1 properly executed her duties pursuant to SECNAV M-5239.1, section 2.4.9.

Conclusion

177. The allegation that between March and April 2013, Subject 1, IAM, Naval Undersea Warfare Center Division Newport, Newport, Rhode Island, falsely reported information assurance vulnerabilities as being "Fully Compliant," or failed to mitigate vulnerabilities in violation of SECNAV M-5239.1, section 2.4.9, is not substantiated.

Observations

178. This investigation highlighted the confusion that can occur without adequate documentation and training for IA

programs/personnel. Although NUWC Division Newport had a standing plan and an underlying SOP, almost 12 months had passed since the latest version was released. During this time, the IA scanning and remediation programs experienced numerous changes.

179. The unclear requirements for OCRS compliance reporting also added to the confusion. There was no clear guidance requiring activities to amend prior OCRS compliance statuses. Those IAVs that reappeared during scans were up to interpretation as to what should happen. The NCDOC SME stated that if monthly scans reveal non-compliance, the Commands should amend their reporting in OCRS. However, in the instance of NUWC Division Newport, OCRS re-reporting would require a considerable amount of effort to report non-compliance due to its daily scanning.

Actions Planned or Taken

180. On 10 January 2014, the NAVSEA Inspector General provided a draft copy of this report to the Commander, NUWC Division Newport. The Commander, NUWC Division Newport was tasked to review the report, and to take any action deemed appropriate.

181. U.S. Fleet Cyber Command has been a collaborator to this investigation since the initial OSC tasking. A final copy of this report will be provided to the Inspector General of U.S. Fleet Cyber Command for review and action deemed appropriate.