Monday, June 30th, 2014

Mr. Jeffrey McDuff
[redacted]
Carol Stream, Illinois 60188

U.S. Office of Special Counsel
1730 M Street, N.W., Suite 218
Washington, D.C. 20036-4505
202-254-3600

RE: OSC File No. DI-13-2697, Whistleblower Comments

Dear Ms. Hryniewicz,

Thank you for the opportunity to review and comment on the agency report and supplemental report conducted by the Department of the Navy on January 16th and May 2nd of this year. Although I take great exception with the overall narrative of the NAVINSGEN investigation I will limit my comments to errors, omissions, and faulty conclusions as it directly relates to the agency report.

On July 28th, 2012 I received the appointment as a member of the Naval Undersea Warfare Center Division, Newport Information Assurance Workforce (IAWF). The appointment states in part;

> *"[Y]ou are hereby appointed as a member of the Division Newport Information Assurance Workforce. As such, you are responsible for ensuring the Information Assurance (IA) related requirements are met for the systems or networks within your cognizance. In addition, you are responsible for reporting to the assigned Information Assurance Officer (IAO) and Information Assurance Manager (IAM) on IA issues affecting those system or networks."*

In addition, the appointment further states:

> *"[Y]our IA duties are at the following category and level: Category: IAM Level: II"*
>
> *"[A]s a condition of your appointment, you are required to obtain and maintain the professional certifications [CISSP] appropriate for your appointment"*

On August 2nd, 2012 the Vulnerability Manager delegated 8 specific tasks prior to his transfer to another position (code 25) within the Naval Undersea Warfare Center Division Newport.

1. Primary reviewer: IA Approval of NAV-IDAS (Navy- Information Dominance Acquisition System)
2. Trainer: Tasked to trair [redacted] as an alternate reviewer
3. NAV-IDAS SOP: Tasked to Draft the Standard Operating Procedures
4. INFOCON 3: Manage the INFOCON Quarterly Exercises (Reported in OCRS)
5. INFOCON 3: Incident Handling (Response)
6. Media Transfer Agent: Overall Program Manager

7. Media Transfer Agent: Policy development, SOPs, Training
8. Training: Train Media Transfer Agents throughout the Command

VARS Scan Results - Throughout the agency report it refers to "VARS Scan Results" as indisputable electronic evidence which is unequivocally false and points to the investigators lack of understand of the technological tools in use at the Naval Undersea Warfare Center Division Newport. eEye Digital Security's Retina Network Security Scanner was the only government authorized vulnerability assessment application used to conduct enterprise-wide vulnerability identification and analysis. The eEye Retina application produces a proprietary Retina Network Scanner Output File with an ".rtd" file extension which is designed to be opened, viewed, and analyzed within the eEye Retina application suite.

The Vulnerability Analysis and Remediation System (VARS) tool is incapable of conducting any scanning activities and therefore cannot produce any scan results! This application was designed, programmed, and implemented by code 1142 contract personnel specifically to reverse-engineer the proprietary eEye Retina ".rtd" output files. They have terms this "parsing" information from the scan results. Throughout the agency report there are references to "VARS Scan Results" with the .xls file extension. This is the product of parsing information from the raw data files produced by the scanning application. The ".xls" is a Microsoft Excel application Workbook file extension specifically designed to manipulate the data found within its workbook pages. My one and only purpose for using the VARS tool was to strip away sensitive information found in the raw data files (.rtd) and transmit via email (.xls) only that information relevant to the conversation.

Critical to this investigation is the triggering event; **the contract dispute**. The contract dispute revealed the fact that the entire vulnerability scanning and reporting process was in the hands of two contract employees. For several weeks after 64 contractors were immediately dismissed no vulnerability scan were conducted by code 1153 employees. I know this to be a fact because I was the lone remaining member of the vulnerability team during the contract dispute and had no administrative access to eEye Retina scanning tools or the VARS application. This was not a typical situation and is evidence of poorly managed internal controls.

As a consequence of the contract dispute the Information Assurance Manager through my direct superviso [redacted] made this request via email on Wednesday, February 6th, 2013:

> *"I would like to see Jeff become more involved with the Vulnerability Scanning and HBSS Review programs which are currently managed and operated by 2 contract personnel, in order to ensure coverage on the govt side as contingency planning."*

Separations of Duties - As a CISSP, I am trained to recognize and adhere to the organizations internal controls. The Separation of Duties in this environment was clearly defined; code 1153 vulnerability team scans, monitors, analyzes, and reports. Code 1142 remediation team members verify, remediate, and report their progress. The fact that there was significant "collaboration" between the two contract employees and the remediation manager invalidates this internal control.

Dynamic Environment - The investigative conclusions that the reappearance of "overdue" IAVA's where simply attributed to the result of a dynamic network environment is a clear subterfuge. The "dynamic environment" conclusion portends that there are no policies, procedures, standards, or internal mechanisms in place to defend against the risk associated with changing a machines configuration, software, and the like in a live computing environment. This is a false conclusion and there were internal policies and procedures in place to reduce or diminish the accordion effect associated with vulnerabilities reappearing after being reported "fully compliant" in the Online Compliance Reporting System (OCRS):

1. **Change Control Board** (CCB) was mandatory in a classified or unclassified enclave/network to receive and maintain its "Authority to Operate" (ATO) per DOD regulations. CCB's are designed to prevent the haphazard practice of installing, updating, or changing a machines software or configuration in a live environment without first testing, evaluating, and approving those changes prior to introducing them into a "dynamic environment."
2. **"Scan, Remediate, Rescan"** are the words used by the investigative teams SME. This is Standard Operating Procedure (SOP) and serves as an internal mechanism to prevent the reappearance/reintroduction of IAVA's, IAVB's, IAVT's, or any other previously unmitigated vulnerability into the computing environment.

The simplest explanation of why previously reported "overdue" vulnerabilities disappeared on one scan only to reappearing on a later scan is that the device was simply powered off! Because of the close collaboration of the remediation manager with the vulnerability team, the well-known automated scanning schedule, and the lack of overnight usage of the computing environment, it was significantly less complicated and economically feasible to simply shut down or disconnect the offending device during the hour's automated eEye Retina scanning took place. The problem arises when an unscheduled (one-off) Retina scan was launched during production hours. This is where you see a reappearance of vulnerabilities previously reported "Fully Compliant."

"2,000 Unmitigated IAVA's" - The investigative team made repeat reference to and concluded that 2,000 unmitigated IAVA's were never found or ever reported being seen by the witnesses they interviewed. The term "IAVA's" was used in it the broader context throughout my tenure. However, there were 2,000 unmitigated "vulnerabilities" as stated in my original Whistleblower complaint. The 2,000 unmitigated vulnerabilities included IAVA's, IAVB's, IAVT's and other known vulnerabilities all individually identified by their eEye Retina audit identification numbers. Even the untrained eye can look at the 47 page 5 April 2013 printout included in the supplemental report and understand why someone would be alarmed at what it represents.

I would like to thank you and the U.S. Office of the Special Counsel for the serious consideration you've shown in this complainant. Unfortunately, it appears the evidence of malfeasance was deleted or destroyed long before investigators were able to make use of it. I must say, in my life to include more than twenty years of decorated military service, I have never worked among of a more apathetic and dysfunctional group of people.

Respectfully,

Jeffrey McDuff