



DEPARTMENT OF VETERANS AFFAIRS

Washington DC 20420

NOV 22 2013

The Honorable Mike Coffman
Chairman
Subcommittee on Oversight and Investigations
Committee on Veterans' Affairs
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Coffman:

Thank you for your letter co-signed with Ranking Member Kirkpatrick dated October 22, 2013, regarding the Department of Veteran Affairs' (VA) efforts to safeguard Veteran information.

We take seriously our obligation to properly safeguard any personal information within our possession. As indicated in our letter of November 8, 2013, in light of the range of questions posed by your letter, we think it is important to subject these matters to an independent review, a function traditionally performed by the VA Office of Inspector General (OIG). As noted, we requested that OIG conduct this independent review in addition to the subject matter under review in their annual audit pursuant to the Federal Information Security Management Act (FISMA) (44 U.S.C § 3544(c)). OIG has yet to respond formally to our formal request. We believe that such an independent review is the best way to address your questions and provide you with complete, objective, and thorough information.

We are also committed to working to provide the Subcommittee with appropriate information while awaiting the results of an independent audit. This letter provides information in response to questions raised in your letter. Additionally an initial CD with requested documents is enclosed. The documents include the handbooks and directives that guide VA's work in the area of data security, and should provide the basis for our continued discussions on this topic. VA will continue to work to provide information that is responsive to the Subcommittee's requests.

Your letter expressed considerable interest in the reporting of data breaches. It is important to note the distinction between data breaches and cybersecurity incidents. A data breach is any security incident that results in the loss, theft, or other unauthorized access to an individual's sensitive personal information, whether electronic or on paper (virtually all of VA's data breaches are paper-based, equipment loss, or unencrypted e-mailing of sensitive information). A cybersecurity incident is a security incident in which an individual has attempted to gain unauthorized access to an information system or systems in the VA network. A cybersecurity incident may or may not lead to a data breach depending on the agency's cybersecurity performance in relation to the incident and nature of the information if compromised. VA reports

The Honorable Mike Coffman

cybersecurity incidents to the Department of Homeland Security (DHS) in accordance with the Federal incident reporting guidelines. VA, per FISMA, reports annually on the adequacy and effectiveness of our cybersecurity program to Congress. We believe that VA is in compliance with FISMA which established the appropriate governing requirements for information security with respect to Federal agencies. Further, the Office of Information Technology (OIT) implements audit controls in accordance with FISMA, using best practices to avoid negative impact to mission critical functions.

Pursuant to FISMA, as outlined in VA Policy VA Handbook 6500, all cybersecurity incidents must be reported to DHS's United States Computer Emergency Readiness Team (US-CERT). Cybersecurity incidents determined to also be a data breach must be reported under FISMA to the US-CERT and under 38 U.S.C. § 5726 to the Committee on Veterans Affairs and the House of Representatives on the quarterly data breach report, along with data breaches that occur but which are not considered cybersecurity incidents. Based on the above requirements, VA has provided US-CERT with notification of all known cyber incidents, and has provided the Committee on Veterans Affairs with all required data breach reports. Neither FISMA nor § 5726 require VA to notify the Committee of cybersecurity breaches that do not result in a data breach.

As referenced in your letter, from January 2010 through October 2013, a total of 29,468 potential data breach incidents were reported. Of those reported incidents, 1,933 tickets were referred to VA's Data Breach Core Team. When VA briefed the House and Senate Veterans' Affairs Committee staff in July 2013, the reported number of incidents for 2013 was current through that point in the calendar year. VA expects that when calendar year 2013 comes to a close, the number of reported incidents will remain consistent with reported numbers for 2012. The apparent decline is due to partial-year results pulled at the time the briefing was given.

VA's current Information Technology (IT) security posture is represented by the Information Operations Conditions (INFOCON) system. INFOCON is an alerting system used to establish a level of vigilance against threats to VA. A scale of "INFOCON Levels" communicates the threat to the VA enterprise and its core mission. VA's current information security posture is considered "elevated," which is explained in further detail below. VA's Network and Security Operations Center in consultation with leadership make this determination on an ongoing basis.

Each of the five INFOCON Levels reflects a defensive posture involving actions to protect VA from risk. Higher threat conditions indicate a greater risk to the enterprise. Risk includes both the probability of an attack occurring and the potential damage to operations, systems, and information. Situation Awareness Reports, Bulletins, or Alerts may be issued to provide specific instructions as needed.

The Honorable Mike Coffman

Effective November 21, 2013, VA raised its INFOCON level from Guarded (Blue) to Elevated (Yellow). This change is in response to an increased number of incidents reported to VA from US-CERT, the annual security risks that accompany the holiday season, and the public's recent interest in VA's information security posture.



Elevated (current security posture)

Indications & Warnings indicate targeting of a specific system, location, unit, or operation

- Significant level of network probes, scans, or activities detected indicating a pattern of concentrated reconnaissance
- Incident occurs at Senior VA Management operating unit that affects a VA Enterprise system or may affect other Senior VA Management operating unit such as a Category 1 Unauthorized Access with a low impact
- Intelligence indicates imminent attack against Senior VA Management operating unit

The information below provides the Subcommittee with detailed information regarding VA's policy and practice regarding addressing security vulnerabilities in Web applications and programs.

VA uses the capabilities explained below to address security vulnerabilities in Web applications and programs. VA uses the results from these scans and programs to make necessary and appropriate changes.

Common Weakness Enumeration (CWE)	Currently in use across the enterprise. VA- Network Security Operations Center (NSOC) has scan engines deployed in the NSOC IP space to conduct vulnerability, Federal Desktop Core Configuration, United States Government Configuration Baseline, content, & Payment Card Industry scanning. Facilities/system owners request scans for ATOs or when new assets are being deployed. Additionally, NSOC scans all facilities as part of a continuous monitoring plan.
Web scanners for Web-based applications	VA uses penetration testing on custom-developed and COTS software being deployed. The testing is comprised of manual penetration testing with tools like web browsers and web proxies. Automated testing uses active scanning tools. The results are submitted to developers for remediation prior to deployment. NSOC conducts penetration testing, application,

The Honorable Mike Coffman

	and web application security assessments for systems being developed and systems renewing accreditation packages.
Common Attack Pattern Enumeration and Classification (CAPEC)	The testing is comprised of manual Web Application Security Assessments & penetration testing with tools like web browsers and web proxies. Automated testing uses active scanning tools. The results are submitted to developers for remediation prior to deployment. NSOC conducts penetration testing, application, and web application security assessments for systems being developed and systems renewing accreditation packages.
Static Code Analysis Tools	Used by Product Development personnel to test code during development. Used by NSOC as independent assessment prior to ATO.
Manual code reviews (especially for weaknesses not covered by the automated tools)	Source Code subject matter experts are being brought on to support manual code reviews.
Dynamic Code Analysis Tools	Combination of tools help to assess easy targets and compliment / validate each other. Usually conducted against pre-production or development instances of applications to reduce impact of testing. Coordinated via system owners, web operations, of the office of cybersecurity.
Web scanners for web-based applications	Combination of tools help to assess low-hanging fruit and compliment / validate each other. Usually conducted against pre-production or development instances of applications to reduce impact of testing. Coordinated via system owners, web operations, of the office of cybersecurity.
PEN testing for attack types not covered by the automated tools.	Manual testing of Web Application Security Assessment Work Program / Open Web Application Security Project top ten. Use web browsers & web proxies. Majority of vulnerabilities are discovered via manual testing. Teams use these checklists and test to enumerate business logic flaws / errors.
Common Weakness Scoring System (CWSS)	Assessment team uses CWSS / CWRAF to score enumerated vulnerabilities based on technical impact and the impact on VA employees to serve Veterans. Majority of assessments are against pre-production / development apps, so the technical impact is actually reduced. We grade based on impact if system contains live / production data / SPI / Financial.

The Honorable Mike Coffman

VA purchased encryption software licenses with the anticipation of encrypting both desktop and laptop computers. VA initially focused on encrypting the latter, due to their portability. Once the Department began encrypting desktops, it first had to ensure that the encryption software was compatible with Windows 7, which was planned for roll-out throughout VA. Testing confirmed that the software is compatible. Subsequently, VA commenced rolling-out Windows 7 with encryption across the enterprise. VA has worked to implement all of the encryption licenses that were purchased. We will purchase more to cover any gaps that may arise as the remaining desktops are encrypted.

With respect to the Windows 7 project as referenced in your letter, the goal is to migrate the majority of all users by November 29, 2013, and identify and migrate any outliers between December 2, 2013, and January 31, 2014. As of October 29, 2013, 87 percent of the VA IT environment, or over 330,000 systems, are running Windows 7.

There may be a small percentage of clients that will not be upgraded by January 31, 2014, due to "blocker" applications. Blocker applications are applications that are not compatible with Windows 7 and have not yet been replaced by the application's owner with a newer version that is Windows 7-compatible. The project team continues to work with application owners to determine the exact number of applications and clients that will not be upgraded by January 31, 2014. These will receive increased attention until upgraded.

As stated in your letter, during testimony at the June 4, 2013, Oversight and Investigations Subcommittee hearing, a recommendation was made to "designate the VA network as a compromised environment" and that VA should "establish controls that are effective and support the reclamation of control back to VA from nation state sponsored organizations."

To our knowledge there is no industry-accepted definition of "compromised environment" as it relates to computer network information security. VA has in place a strong, multi-layered defense to combat evolving cybersecurity threats. These defenses include monitoring outside our network by external partners; active scanning of Web applications and source code; and protection of servers, workstations, network, and gateways, among other security efforts.

With regard to your question on a "compromised environment" and domain controls, VA has experienced network incidents as discussed in greater detail during a briefing to your staff on July 12, 2013. VA followed its established standard operating policies and procedures to maintain system integrity. All known computers possibly subject to the incidents were removed from the network and cleaned. Usernames and passwords were reset for all suspected affected users. The Network Security

Enclosed: In a letter dated October 22, 2013, the Honorable Mike Coffman, Chairman of the House Veterans Affairs - Subcommittee on Oversight and Investigations, and Ranking Member Kirkpatrick requested information concerning data security. The requested information is enclosed on a CD.

For Questions 3,4,5,6 in the second part of the Joint letter.

In regards to questions that reference VA Handbook 6500.4, VA notes that this Handbook was a draft that was never published. Relevant requirements from the drafted Handbook were subsequently incorporated into both VA Directive and VA Handbook 6500. Furthermore, VA asserts that the reference to the draft VA Handbook 6500.4 is actually an incorrect reference, because this handbook, as originally drafted, dealt exclusively with patch and vulnerability management and did not contain any reference to reporting or submitting of information to the Secretary of Veterans Affairs. In an effort to provide relevant documentation to the requests in the letter dated 10/22/13, VA has submitted copies of the Quarterly Incident Reports, Monthly Incident Reports, and Weekly Incident Reports to demonstrate items which are reported to agency officials in accordance with VA Directive 6500.

For Question 8 in the second part of the Joint Letter

The term "compromised," as referenced in the letter dated 10/22/13 and as defined in NIST SP 800-32 - *Introduction to Public Key Technology and the Federal PKI Infrastructure (National Institute of Standards & Technology)*, FIPS Pub 140-2 - *Security Requirements for Cryptographic Modules (Federal Information Processing Standards)*, and CCSSI-4009 - *National Information Assurance (IA) Glossary*, is overly broad. It is taken out of context because the references apply to cryptographic systems or processes. As defined in the above mentioned references, the term "compromised" could be construed to indicate all incidents, electronic or paper, in the attached Weekly Incident Reports, Monthly Incident Reports, and Quarterly Incident Reports.

Please sign and date below to acknowledge receipt. Thank you.

Signature: 

Printed Name: BEN FENDER

Title: ~~MEMBER~~ FELLOW

Committee: HVAC

Date: 22 NOV 2013

Delivered by: MATT SANTOS