VA Office of Inspector General

OFFICE OF AUDITS AND EVALUATIONS

Department of Veterans Affairs

Review of Alleged Breach of Privacy and Confidentiality of Personally Identifiable Information at the Milwaukee VARO

September 15, 2016
16-00623-306

ACRONYMS

CVSO	County Veterans Service Organization
MOU	Memorandum of Understanding
OI&T	Office of Information and Technology
OIG	Office of Inspector General
PII	Personally Identifiable Information
SSN	Social Security Number
TVSO	Tribal Veterans Service Organization
VA	Department of Veterans Affairs
VARO	VA Regional Office
VBA	Veterans Benefits Administration
VSO	Veterans Service Organization
WDVA	Wisconsin Department of Veterans Affairs

To report suspected wrongdoing in VA programs and operations, contact the VA OIG Hotline:

Web Site: www.va.gov/oig/hotline

Email: vaoighotline@va.gov

Telephone: 1-800-488-8244

Highlights: Review of Alleged Breach of Privacy and Confidentiality of PII at VBA's Milwaukee VARO

Why We Did This Review

In October 2015, the Office of Inspector General (OIG) received a request from U.S. Senators Richard Blumenthal and Tammy Baldwin to review an incident concerning the improper dissemination of veterans' personally identifiable information (PII) by a Wisconsin Department of Veterans Affairs (WDVA) employee to an unauthorized recipient over VA's email server.

What We Found

We substantiated the allegation that on April 1, 2015, a WDVA employee improperly disseminated a monthly claims report over VA's email server. The report contained updates of Wisconsin veterans' disability claims, to unaccredited County and Tribal Veterans Service Organization employees not authorized to handle sensitive information, as well as to a Wisconsin veteran. The Milwaukee VA Regional Office (VARO) sharing of claims information with WDVA was consistent with Federal policy.

This incident occurred because VA did not have adequate processes and information security controls in place to safeguard against unauthorized disclosure of PII. The VA Office of Information and Technology (OI&T) did not adequately configure VA's information security filtering software to block the dissemination of unencrypted sensitive data before releasing information to WDVA. In addition, the VARO did not have a formal agreement with WDVA for sharing PII. As a result, VA put Wisconsin veterans' PII at unnecessary risk of interception and misuse.

Furthermore, our audit of VA's Federal Information Security Modernization Act Audit for Fiscal Year 2015 reported security deficiencies similar in type to those identified in this report as material weaknesses over the last few years.

What We Recommended

We recommended the Assistant Secretary for Information and Technology improve VA's email security filtering software controls, establish formal agreements with third-party organizations, evaluate whether permanent encryption controls are needed for non-VA employees with VA accounts, and conduct reviews of processes and controls at VAROs collaborating with third-party organizations, to ensure security of sensitive veterans' information.

Agency Comments

The Assistant Secretary for Information and Technology nonconcurred with our recommendations and stated that VA's position was unchanged since its response in February 2016 to the Senate Committee on Homeland Security and Governmental Affairs. The Assistant Secretary believed that all policies, procedures, and required training were already in place. However, we maintain our position that VA did not have adequate processes and information security controls in place to safeguard against unauthorized disclosure of PII.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

TABLE OF CONTENTS

INTRODUCTION

Allegation

In October 2015, the Office of Inspector General (OIG) received a request from U.S. Senators Richard Blumenthal and Tammy Baldwin to review an incident concerning the improper dissemination of veterans' personally identifiable information (PII), by a Wisconsin Department of Veterans Affairs (WDVA) employee at the Milwaukee VA Regional Office (VARO), to an unauthorized recipient. The sensitive information was disseminated over VA's email server. The request involved determining whether VA's processes and systems for sharing information with non-agency personnel were adequate to safeguard veterans' PII.

Background

The Veterans Benefits Administration (VBA) has 56 VAROs that process disability claims and provide services to veterans and their families. The Milwaukee VARO has six Veterans Service Organizations (VSOs) located onsite, one of which is WDVA. WDVA acts as a liaison to help Wisconsin veterans facilitate the timely adjudication of their disability claims filed with VA. Under WDVA, there are 72 County VSOs (CVSOs) and 11 Tribal VSOs (TVSOs) that provide information and assistance to Wisconsin veterans seeking Federal and state benefits and services.

Prior Reviews

OIG's "*Review of Alleged Transmission of Sensitive VA Data Over Internet Connections"* (Report No. 12-02802-111, March 6, 2013) substantiated an allegation that VA was transmitting sensitive data, including PII and internal network routing information, over unencrypted telecommunications carrier networks. We found that Office of Information and Technology (OI&T) management was aware of this practice and accepted the security risk of potentially losing or misusing the sensitive information exchanged, via a waiver. Without controls to encrypt the transmission of sensitive VA data, veterans' information might be vulnerable to interception and misuse by malicious users as it traverses unencrypted telecommunications carrier networks. Furthermore, malicious users could obtain VA router information to identify and disrupt mission-critical systems.

Other Information

- Appendix A provides details on our scope and methodology.
- Appendix B provides comments by the Assistant Secretary for Information and Technology.

RESULTS AND RECOMMENDATIONS

Finding

VA's Processes and Controls Allowed the Dissemination of Wisconsin Veterans' PII to Unauthorized Recipients

We substantiated the allegation that on April 1, 2015, a WDVA employee improperly disseminated over VA's email server a monthly claims report that contained updates on Wisconsin veterans' disability claims to unaccredited CVSO and TVSO employees not authorized to handle sensitive information, as well as to a Wisconsin veteran. The employee obtained the report from the Milwaukee VARO, which contained PII, including 638 names along with 416 Social Security Numbers (SSNs) and 222 claim numbers of Wisconsin veterans. While we determined that the VARO's sharing of claims information with WDVA was consistent with Federal policy, WDVA staff did not need the report to help veterans facilitate the timely adjudication of their disability claims filed with VA. Furthermore, we determined that the improper dissemination of PII over VA's email server was a violation of the Federal Information Security Management Act.

This incident occurred because VA did not have adequate processes and information security controls in place to safeguard against unauthorized disclosure of PII. OI&T did not adequately configure VA's information security filtering software to block the dissemination of unencrypted sensitive data before releasing information to WDVA. In addition, the Milwaukee VARO did not have a formal agreement, such as a Memorandum of Understanding (MOU), with WDVA for information sharing that described their respective responsibilities. This includes the specific PII shared with WDVA, such as the claims report, the purposes for which PII may be used, and the VARO's monitoring of WDVA employees' network activity on VA's email server. As a result, VA put Wisconsin veterans' PII at unnecessary risk of interception and misuse.

WDVA Internal Investigation

On April 7, 2015, WDVA initiated an internal investigation into the April 1, 2015 data breach incident. The investigation determined that a Milwaukee VARO employee sent an email to a WDVA claims director and a supervisor with an attached claims report that contained a status update on disability claims for 637 Wisconsin veterans.[1] The email was sent over VA's network using the WDVA director's and the supervisor's VA email accounts. According to WDVA's Division Administrator, the former WDVA director established unofficial and undocumented procedures for

[1] The director and supervisor both resigned before the start of our review in November 2015. In addition, our review found that the claims report contained data for 638 veterans instead of 637.

sending the claims report to CVSOs and TVSOs. The director would first redact sensitive information from the report received from the Milwaukee VARO and then send the redacted version to the supervisor with instructions to forward the report to CVSOs and TVSOs. The investigation determined that the WDVA staff routinely shared VA-redacted disability claims reports with unaccredited CVSO and TVSO staff since June 2014.

OIG Review

The former WDVA supervisor reported that on April 1, 2015, he edited the distribution list to remove a contact who no longer worked as a CVSO. During that process, the supervisor accidentally pressed a keyboard letter causing the auto-complete feature of Microsoft Outlook to auto-populate an unauthorized veteran's email address to the distribution list. The supervisor then removed the email encryption, and using their VA email accounts, sent the claims report to 186 recipients who could not open encrypted emails. The recipients included unaccredited CVSO and TVSO employees and the unauthorized Wisconsin veteran.

Of the 186 email recipients who received the report, 39 (21 percent) were unaccredited CVSO and TVSO employees. The responsible WDVA staff had not classified an additional 29 recipients (16 percent) as accredited or unaccredited staff. According to Federal regulations, a recognized organization shall file with VA's Office of General Counsel the application for accreditation as a service organization representative for a designee that may represent claimants for VA. Without the accreditation, VSO employees are not authorized to handle sensitive information, including assisting veterans with the preparation, presentation, and prosecution of a claim for VA benefits.

A WDVA supervisor reported that he did not understand why the former director would send the claims report containing 638 Wisconsin veterans' information to all CVSOs and TVSOs. The former director should have only sent the claims report information for a particular veteran to the appropriate veteran's accredited CVSO or TVSO. However, we concluded that WDVA's investigation incorrectly determined that the incident occurred because Milwaukee VARO's email security software that detects sensitive data, such as SSNs, malfunctioned and did not provide a warning to the sender or block the inappropriate dissemination of PII.

Why Filter Did Not Block Veterans' PII

The security filter did not block the improper transmission of Wisconsin veterans' PII because OI&T did not configure the security filter to identify the phrase "file number," or to flag nine-digit numbers without delimiters. The VARO's monthly claims report includes a column labeled "file number," that contains SSNs and claim numbers. The report lists the SSNs as nine-digit numbers without delimiters. For example, the security filter would not flag a veteran's SSN transmitted without dashes, such as 123456789.

The Associate Director, VA's Service Design and Implementation, indicated that they did not configure the security filter to flag nine-digit numbers without delimiters because other VA business functions use nine-digit numbers such as contracts, support tickets, and classes. In addition, if the filter flagged all nine-digit numbers transmitted by email, it would prevent the dissemination of appropriate emails. Ultimately, OI&T's security filter configuration allowed WDVA staff to transmit unencrypted emails containing Wisconsin veterans' PII to unintended and unauthorized recipients over VA's email server.

In December 2015, VA's Network Security Operations Center staff began testing a data loss prevention feature to improve the email security filter. OI&T tested the improved filter to search for nine-digit number strings, provided keywords or phrases exist. According to VA's Associate Director, Service Design and Implementation, the test's success rate more than doubled, while false positives were near zero. Although OI&T improved the security filter, there are potential number strings OI&T might not be aware of that the filter does not flag for review. Without the proper filter setting, there is a risk that unauthorized disclosure of veterans' sensitive information, including PII, could result in misuse.

No MOU Between VA and WDVA

The Milwaukee VARO did not maintain an MOU or other agreements with WDVA specifying VA network usage rules, protection of PII, or appropriate oversight by the VARO. The VARO IT Chief indicated that an MOU with WDVA was unnecessary because the WDVA employees who had access to VA's network were subject to the same security and privacy awareness training and National Rules of Behavior as VA employees.

WDVA employees used VA's network to transmit veterans' information to external organizations such as CVSOs and TVSOs. Although both WDVA employees and VA employees are required to take the same security and privacy training and sign the same rules of behavior annually to maintain access to VA's network, an MOU is needed to further define information security requirements, the network architecture, the types of data exchanged, and the appropriate roles and responsibilities. Therefore, VA should establish an MOU with WDVA to ensure WDVA officials institute information security controls commensurate with VA standards. The requirement for establishing MOUs are found in these publications:

- The Federal Information Security Management Act requires agencies to implement National Institute of Standards and Technology guidance and standards. Specifically, the National Institute of Standards and Technology Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, states that if an organization shares PII, the organization should implement the appropriate documented agreements for roles and responsibilities, restrictions on further sharing of PII, minimum security controls, and

other relevant factors. These agreements ensure that the partner organizations abide by rules for handling, disclosing, sharing, transmitting, retaining, and using the organization's PII.

- VA Handbook 6500, *Risk Management Framework for VA Information Systems–Tier 3: VA Information Security Program* states that MOUs are required, where appropriate, for information sharing with third parties that specifically describe the PII covered and the purposes for which PII may be used. The Handbook further states that VA is required to monitor the authorized uses and sharing of PII with third parties.

The Milwaukee VARO Information Security Officer indicated that officials were unaware of their responsibility for monitoring WDVA employees' activity on the VA network. However, the Information Security Officer later agreed that a written agreement between the VARO and WDVA detailing the VARO's level of controls over WDVA's VA network activity would be helpful to establish a clear and effective oversight.

Effect of Inadequate Processes and Controls

If VA's processes and information security controls are not improved, VA might be unaware that PII and other sensitive information could potentially be shared with unintended and unauthorized recipients. In addition, the confidentiality, integrity, and availability of veterans' PII and other sensitive information will remain at risk of unauthorized disclosure or misuse. Ultimately, the consequence of inadequate information security controls over veterans' PII may be veterans' loss of trust in VA.

WDVA Policy Updates

According to the WDVA Division Administrator, before the data breach incident in April 2015, WDVA did not have a written policy on how to handle the improper transmission of PII by their employees. However, following the incident, WDVA Chief Legal Counsel told us that they had reviewed all of its internal and external policies and made improvements to their protocols for protecting Wisconsin veterans' sensitive information, including PII. Specifically, WDVA:

- Terminated the transmission of claims reports to CVSOs and TVSOs
- Disabled the Microsoft Outlook auto-populate feature
- Created a Privacy and Security Policy
- Instituted a Privacy and Security Officer to conduct internal audits, policy overviews, and training
- Updated Technology Use Policy with privacy and security protocols
- Required the use of Personal Identity Verification cards and encrypted email communication across the CVSO and TVSO community

WDVA developed new policies and training internally to improve its security posture and awareness. We were told that all WDVA staff at the

Milwaukee office received updated privacy and security training to help emphasize their responsibilities, expected behavior, and duty to protect veterans' information. According to WDVA legal counsel, WDVA needed stronger controls to protect veterans' sensitive information. WDVA legal counsel also agreed that an MOU with VA and non-VA employees on the privacy and security rules and practices would be helpful in specifying the roles and responsibilities of VA and WDVA. Although WDVA implemented new policies on protecting sensitive information, we did not test those policies nor did we provide an opinion on their effectiveness because WDVA is a State agency and OIG does not have authority over WDVA's internal operations.

Conclusion

Given VA's partnership and sharing of data with WDVA to assist veterans with the preparation, presentation, and prosecution of their claims for VA benefits, VA must ensure information system controls and that all users protect veterans' PII and other sensitive information. OI&T did not adequately configure VA's email security filter to block a WDVA employee's improper transmission of Wisconsin veterans' PII over VA's email server. In addition, WDVA's method of information sharing with third parties left veterans' PII vulnerable to potential unauthorized access, loss, or disclosure. WDVA also did not have adequate processes and procedures for transmitting veterans' PII to third-party organizations. The security deficiencies identified in this report are similar in type to those reported in our audit of VA's Federal Information Security Modernization Act Audit for Fiscal Year 2015 as material weaknesses over the last few years.

Recommendations

1. We recommended the VA Assistant Secretary for Information and Technology improve VA's email security filtering software configuration controls to effectively flag improper transmissions of veterans' personally identifiable information over the VA network.

2. We recommended the VA Assistant Secretary for Information and Technology establish formal agreements with third-party organizations that define network responsibilities, processes, and procedures for handling sensitive veterans' information, and require that information security controls be implemented commensurate with VA's information security standards.

3. We recommended the VA Assistant Secretary for Information and Technology evaluate whether permanent encryption controls are needed for non-VA employees who maintain VA accounts for conducting business on behalf of veterans.

4. We recommended the VA Assistant Secretary for Information and Technology conduct reviews of processes, procedures, and controls in place at VA regional offices that collaborate with third-party organizations to ensure security of sensitive veterans' information.

Management Comments

The Assistant Secretary for Information and Technology nonconcurred with all four recommendations and stated that VA's position was unchanged since its response in February 2016 to the Senate Committee on Homeland Security and Governmental Affairs (included as Attachment 2 of the memo from the Assistant Secretary for Information and Technology – Appendix B of this report). According to the Interim Chief of Staff who signed the response, it was perfectly legal for VA to provide WDVA a spreadsheet of recently closed claims that contained 638 veterans' names and SSNs. The Interim Chief of Staff also stated that the event regarding the improper transmission of Wisconsin veterans' PII did not represent a breach or failure on the part of VA. Instead, the Interim Chief of Staff stated it was an inadvertent release of PII that resulted from human error for which WDVA accepted responsibility.

The Assistant Secretary believed that all policies, procedures, and required training were already in place. Furthermore, she went on to state that a memo would be sent to all VA executive leaders reminding them of the importance of completing the annual mandatory VA Privacy and Information Security Awareness training and stressing that information security must be incorporated into all VA processes and procedures. As a result, the Assistant Secretary requested closure of Recommendations 1 through 4.

OIG Response

We disagree with OI&T's assertion that the improper dissemination of veterans' PII over VA's email server to unauthorized recipients was not a data breach and that adequate controls were already in place. We never had an issue with whether VA's sharing of information about veterans' claims with WDVA was legal. Our concern is whether VA's data governance approach was effective in ensuring that third-party organizations adequately controlled and protected veterans' PII. VA does not address the important point that leaving third-party organizations responsible for data governance without coordinated VA oversight has proven ineffective.

Although the Assistant Secretary nonconcurred with Recommendation 1, her response stated that VA's email filtering software was updated and strengthened to flag the improper dissemination of veterans' PII over the VA network. Specifically, VA strengthened the calibration in the scanning tool to include additional words and phrases that expanded the capability to detect PII. In addition to strengthening the scanning tool, there will be an ongoing effort by OI&T's security staff to analyze traffic traversing VA's boundary to identify potential SSNs embedded in transmissions. This effort will help the security staff build custom filters to limit the risk of inappropriate data transmissions. The actions taken to improve VA's email filtering software

and the ongoing analysis of email transmissions to identify potential scenarios that could compromise veteran's PII addressed Recommendation 1. Therefore, we determined the evidence provided was sufficient to close Recommendation 1.

For Recommendations 2 through 4, the Assistant Secretary did not directly address the recommendations but instead referenced her response to Recommendation 1, which stated that VA's position was unchanged since their February 2016 response to the Senate Committee on Homeland Security and Governmental Affairs. However, for Recommendation 2, the report clearly shows VA does not maintain adequate policies and procedures over VSOs authorized to use VA's network. For example, because WDVA used VA's network to transmit veterans' information to CVSOs and TVSOs, the VARO should have established an MOU with third-party organizations to help with transparency and clearly define information security requirements, network architecture, types of data exchanged, and appropriate roles and responsibilities. In addition, an MOU is one means of documenting data sharing agreements and ensuring VA partners institute information security controls commensurate with VA standards.

Regarding Recommendation 3, the Assistant Secretary did not provide support for why permanent encryption controls were not needed for non-VA employees who maintained VA accounts to conduct VA business. Non-VA employees, such as WDVA employees, maintained their own State email accounts, in addition to maintaining VA email accounts. We maintain our position that permanent encryption controls on VA accounts for non-VA employees would be a reasonable added control to protect against the improper dissemination of veterans' PII.

Recommendation 4, concerned conducting reviews of processes, procedures, and controls in place at VAROs that collaborate with third-party organizations to ensure security of sensitive veterans' information. Even though WDVA accepted responsibility for improperly disseminating veterans' PII in April 2015, VA was responsible for ensuring information system controls, and all users of the VA network protect veterans' PII and other sensitive information at all levels, including third-party organizations. While it was legal for the VARO to send a monthly disability claims report to WDVA recipients, the VARO discontinued the practice of sending the report to WDVA after the data breach occurred.

The action taken by the VARO did not negatively affect WDVA's ability to help veterans facilitate the timely adjudication of their disability claims filed with VA. While non-VA users must maintain a heightened and constant awareness of their responsibilities regarding the protection of VA information, VA Handbook 6500 states that VA must achieve the Gold Standard in data security. According to VA Handbook 6500, the Gold Standard requires that VA information and information system users protect

VA information and information systems, especially the personal data of veterans, their family members, and employees. Achieving the Gold Standard means going beyond what is simply legal to conducting routine reviews of processes, procedures, and controls to ensure data security.

Appendix A Scope and Methodology

Scope

We conducted our review from November 2015 to March 2016. The review focused on VA processes, procedures, controls, and systems for protecting the dissemination of veterans' PII over VA's network. We also reviewed WDVA's policies and procedures for properly handling and safeguarding veterans' PII.

Methodology

In December 2015, we conducted site visits at the Milwaukee VARO and OI&T. We interviewed VARO and WDVA officials as well as staff, and OI&T officials to gain an understanding of existing data transmission practices and associated security controls. In addition, we evaluated VA policies, procedures, and information security controls for the transmission of sensitive data over VA networks and related data loss prevention tools. We also interviewed the veteran who was the recipient of unauthorized Wisconsin veterans' PII from the WDVA. Furthermore, we interviewed an attorney from VA's Office of General Counsel to gain an understanding of VA's accreditation process for service organization representatives to gain access to veterans' personal and confidential information.

Data Reliability

Computer-generated data were obtained during this review to support the standard recipients of the disability claims report and the WDVA's maintained listing of accredited and unaccredited CVSO and TVSO staff. We found this listing to be incomplete since it did not contain all standard CVSO and TVSO recipients of the disability claims report. However, based on the intended purpose of the computer-generated data, we determined that it was sufficiently reliable within the context of our review objective.

Government Standards

We conducted this review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

Appendix B Management Comments

Department of Veterans Affairs Memorandum

Date: March 18, 2016

To: Assistant Sectretary for Information and Technology (005)

Subject: Draft Report, Review of Alleged Breach of Privacy and Confidentiality of Personally Identifiable Information (Pll) at the Milwaukee VA Regional Office (VARO) Project Number 2016-00623-DV-0037

1. Thank you for the opportunity to provide our comments to your draft report regarding the improper transmission of Wisconsin Veterans' personally identifiable information (Pll) over Department of Veterans Affairs (VA) servers. Regarding the incident referenced in your draft report, VA's position on this incident is unchanged since our February 2, 2016, response to Senator Johnson, Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs.

2. I have reviewed your four recommendations and believe that all policy, procedures, and required training are already in place. VA Handbook 6500, Risk Management Framework for VA Information Systems and all users of VA IT systems, and/or those having access to sensitive information, must be enrolled in the Talent Management System (TMS), and complete the VA Privacy and Information Security Awareness Training and Rules of Behavior (VA 10176) on an annual basis. I will be sending the attached memorandum to all VA executive leaders to remind them of the importance of completing the mandatory training, but also to stress to them that information security must be incorporated into all VA processes and procedures.

3. VA has strengthened the calibration in the scanning tool to include additional words and phrases that will expand the capability to detect Pll. However, blocking all nine digit numeric patterns without additional factor matching is impracticable, as other non- Pll nine digit numeric patterns are necessary for daily VA support, such as ticket numbers, file tracking, and Outlook meetings notifications. While this re-calibration will result in more "false-positives", VA attempts to manage risk by taking a measured approach, but will always defer on the side of information security.

4. We appreciate your time and attention to our information security program. If you have any questions, feel free to call me at 202-461-6910 or feel free to have a member of your staff contact Susan Perez, Chief of Staff, Office of Information Security (005R), at 202-632-9070.

(original signed by:)

LAVERNE H. COUNCIL

Attachments*

** Due to the number and length, not all attachments were included in this report. Copies may be obtained from the OIG Information Officer.*

For accessibility, the format of the original document has been modified to fit in this document.

Attachment 1

U.S. Department of Veterans Affairs
Office of Information and Technology (OI&T)
Comments on OIG Draft Report:
"Review of Alleged Breach of Privacy and Confidentiality of Personally Identifiable Information (PII) at the Milwaukee VA Regional Office (VARO)"
Project Number 2016-00623-DV-0037

Recommendation 1:	**We recommended the VA Assistant Secretary for Information and Technology improve VA's email security filtering software configuration controls to effectively flag improper transmissions of veterans' personally identifiable information over the VA network.**
OIG Comment:	**04-21-16 Comment:**
OI&T Response:	**Non-concur.** Regarding the incident referenced in your draft report, VA's position on this incident is unchanged since our February 2, 2016, response to Senator Johnson, Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs. I have reviewed your four recommendations and believe that all policy, procedures, and required training are already in place. VA Handbook 6500, Risk Management Framework for VA Information Systems and all users of VA IT systems, and/or those having access to sensitive information, must be enrolled in the Talent Management System (TMS), and complete the VA Privacy and Information Security Awareness Training and Rules of Behavior (VA 10176) on an annual basis. I will be sending the attached memorandum to all VA executive leaders to remind them of importance of completing the mandatory training, but also to stress to them that information security must be incorporated into all VA processes and procedures. VA has strengthened the calibration in the scanning tool to include additional words and phrases that will expand the capability to detect PII. However, blocking all nine digit numeric patterns without additional factor matching is impracticable, as other non-PII nine digit numeric patterns are necessary for daily VA support, such as ticket numbers, file tracking, and Outlook meetings notifications. While this re-calibration will result in more "false-positives", VA attempts to manage risk by taking a measured approach, but will always defer on the side of information security. Target Completion Date: No further action.
Supporting Documentation:	1. Memoranda from the Department of Veterans Affairs, Interim Chief of Staff, on February 2, 2016, to Chairman Ron Johnson, and Ranking Member Thomas R. Carper, Committee on Homeland Security and Governmental Affairs. 2. Memorandum from the Department of Veterans Affairs, Assistant Secretary for Information and Technology, to Under Secretaries, Assistant Secretaries, and Other Key Officials, on "Information Security and Privacy Awareness Training Requirement (VAIQ# 7699332)," dated May 18, 2016. 3. Web-Based Training Storyboard, "FY16 VA Annual Privacy and

	Information Security Awareness and Rules of Behavior." 4. VA Office of Inspector General Report Number 14-04945-413, "Review of Alleged Data Sharing Violations at Palo Alto VA Health Care System," dated September 28, 2015.
Status:	We request closure of this recommendation based on the evidence provided above.

Recommendation 2:	**We recommended the VA Assistant Secretary for Information and Technology establish Memoranda of Understandings with third party organizations that define network responsibilities, processes and procedures for handling sensitive veterans' information, and require information security controls are implemented commensurate with VA's information security standards.**
OIG Comment:	**04-21-16 Comment**:
OI&T Response:	**Non-concur.** OI&T response to this recommendation is addressed in Recommendation 1.
Status:	We request closure of this recommendation based on the evidence provided above.

Recommendation 3:	**We recommended the VA Assistant Secretary for Information and Technology evaluate whether permanent encryption controls are needed for non-VA employees who maintain VA accounts for conducting business on behalf of veterans.**
OIG Comment:	**04-21-16 Comment**:
OI&T Response:	**Non-concur.** OI&T response to this recommendation is addressed in Recommendation 1.
Status:	We request closure of this recommendation based on the evidence provided above.

Recommendation 4:	**We recommended the VA Assistant Secretary for Information and Technology conduct reviews of processes, procedures, and controls in place at VA regional offices that collaborate with third party organizations to ensure security of sensitive veterans' information.**
OIG Comment:	**04-21-16 Comment**:
OI&T Response:	**Non-concur.** OI&T response to this recommendation is addressed in Recommendation 1.
Status:	We request closure of this recommendation based on the evidence provided above.

Attachment 2

DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON DC 20420

February 2, 2016

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Thank you for your October 28, 2015, letter regarding the improper transmission of Wisconsin Veterans' personally identifiable information (Pll) over Department of Veterans Affairs (VA) servers. Please know that VA considers its responsibility to protect Veterans' Pll to be one of the most important aspects of our service.

Regarding the incident referenced in your letter, VA routinely shares information about Veterans' claims, as permitted by the Privacy Act and the title 38 statute that protects claims files, with Veterans Service Officers (VSO) and other individuals who have been designated by Veterans to assist with their claims. 5 United States Code (U.S.C.); § 552a(b)(3); 38 U.S.C. § 5701(b)(1). To that end, on April 1, 2015, an employee of the Veterans Benefits Administration sent to VSOs at the Wisconsin Department of Veterans Affairs (WDVA) a spreadsheet that identified 638 Veterans whose claims had recently been closed. Because the spreadsheet contained the Veterans' names and social security numbers (SSN), the email was encrypted before transmission, in accordance with VA policy and standards established by the National Institute of Standards and Technology (NIST),VA Handbook 6500, Risk Management Framework for VA Information Systems-Tier 3: VA Information Security Program; Federal Information Processing Standards 140-2, Security Requirements for Cryptographic Modules.

Shortly thereafter, we understand that one of the VSOs who received the spreadsheet from VA forwarded that email to a number of state and county VSOs so that they may reach out and offer their assistance to the listed Veterans. Since the recipients were not affiliated with VA and did not have VA email addresses to which encrypted emails could be sent, the VSO's message was, by necessity, sent unencrypted. In addition, although VA's email and network security tools and procedures generally prevent the emailing of Pll without encryption, this transmission was successful because the content did not meet the criteria under the complex rule used by the software, which requires a match of a SSN pattern and a second factor from a list of terms in a text dictionary file that may indicate Pll. Unfortunately, the recipients included a Veteran who is not a VSO or a representative of any of the listed individuals. Although we cannot comment on state and other laws governing disclosure of information by WDVA, we understand that there was no legal authority for the disclosure of this information to the Veteran.

While it was perfectly legal for VA to send the information to the WDVA recipients with the attachment, VA has strengthened the calibration in the scanning tool to include additional words and phrases that will expand the capability to detect Pf I. However, blocking all nine digit numeric patterns without additional factor matching is impracticable, as other non-Pll nine digit numeric patterns are necessary for daily VA support, such as ticket numbers, file tracking, and Outlook meetings notifications. While this re-calibration will result in more "false-positives," VA attempts to manage risk by taking a measured approach, but will always defer on the side of information security.

On April 3, 2015, an investigation was launched and tracked in VA's Privacy Security Event Tracking System. The VA Data Breach Services team investigation determined that the inadvertent release of Pll resulted from human error, and not from failure of VA policy or system security. WDVA accepted responsibility for this human error, and has provided credit monitoring for all individuals whose information was involved in this incident. All users of VA information systems are required to take an annual training on the use and handling of Pll. They also must read and accept VA's National Rules of Behavior governing the use of VA information systems to include the encryption of email containing sensitive Veteran information.

On a related note, prior to the issuance of the Office of Inspector General's (OIG) audit, on December 24, 2012, VA's Office of Information and Technology (OIT) directed a review to ensure that no VA networks are transmitting unprotected sensitive data over public Internet connections. VA validated that Pll was only transmitted over its private network and not a public network. Therefore, while VA disagreed with the assertion made in the March 2013 OIG audit that Pll was being transmitted over the public Internet, VA did concur with the recommendation to perform a

review of VA networks transmitting sensitive data. OIT continues to implement evolving technical configuration controls to ensure encryption of such data is in accordance with applicable VA and Federal information security requirements.

While we regret that the Veterans' information was ultimately misdirected, it is important to note that, with respect to the initial disclosure, VA was legally permitted to share the spreadsheet with WDVA and did so in a way that is compliant with both VA and NIST data security standards. Although the potential compromise to the Veterans' information could have been avoided by the removal of their SSNs from the spreadsheet prior to the subsequent transmission by WDVA to the non-VA recipients, because that communication occurred after the information was properly disclosed outside VA, that event does not represent a breach of VA information or a failure of VA to protect the confidentiality and security of Veterans' information.

VA is grateful for your continuing support of Veterans and appreciates your efforts to pass legislation enabling VA to provide Veterans with the high-quality care they have earned and deserve. As the Department focuses on ways to help provide access to health care in your district and state and across the country, we have identified a number of necessary legislative items that require action by Congress in order to best serve Veterans.

Flexible budget authority would allow VA to avoid artificial restrictions that impede our delivery of care and benefits to Veterans. Currently, there are over 70 line items in VA's budget that dedicate funds to a specific purpose without adequate flexibility to provide the best service to Veterans. These include limitations within the same general areas, such as health care funds that cannot be spent on health care needs and funding that can be used for only one type of Care in the Community program, but not others. These restrictions limit the ability of VA to deliver Veterans with care and benefits based on demand, rather than specific funding lines.

VA also requests your support for the Purchased Health Care Streamlining and Modernization Act. This legislation would allow VA to contract with providers on an individual basis in the community outside of Federal Acquisition Regulations, without forcing providers to meet excessive compliance burdens. Already, we have seen certain nursing homes not renew their agreements with VA because of these burdens, requiring Veterans to find new facilities for residence. VA further requests your support for our efforts to recruit and retain the very best clinical professionals. These include, for example, flexibility for the Federal work period requirement, which is not consistent with private sector medicine, and special pay authority to help VA recruit and retain the best talent possible to lead our hospitals and health care networks.

We appreciate your commitment to keeping our Veterans' data safe and secure and look forward to continuing to work with your office on this matter. Should you have further questions, please have a member of your staff contact Ms. Mandy Hartman, Congressional Relations Officer, at (202) 461-6416 or by e-mail at Mandy.Hartman@va.gov. A similar response has been sent to Senator Carper.

Thank you for your continued support of our mission.

Sincerely,

(original signed by:)

ROBERT D. SNYDER
Interim Chief of Staff

For accessibility, the format of the original document has been modified to fit in this document.

Appendix C OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Acknowledgments	Al Tate, Director Loralee Bennett Christopher Scrabis Daniel Zachareas

Appendix D Report Distribution

VA Distribution

Office of the Secretary
Veterans Health Administration
Veterans Benefits Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans Appeals

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Government Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget
U.S. Senate: Tammy Baldwin, Richard Blumenthal, Ron Johnson
U.S. House of Representatives: Sean P. Duffy, Glenn Grothman, Ron Kind, Gwen Moore, Mark Pocan, Reid Ribble, Paul D. Ryan, James F. Sensenbrenner

This report is available on our Web site at www.va.gov/oig.