Department of Veterans Affairs
Office of Inspector General

Administrative Investigation
Improper Use of Web-based Collaboration Technology
Office of Information and Technology

Redacted

Report No. 13-03054-463 **August 17, 2015**

VA Office of Inspector General
Washington, DC 20420

DEPARTMENT OF VETERANS AFFAIRS
Office of Inspector General
Washington, DC 20420

TO: VA Chief of Staff

SUBJECT: Administrative Investigation, Improper Use of Web-based Collaboration Technology, Office of Information and Technology (OIT) (2013-03054-IQ-0155)

Summary

We substantiated that VA employees improperly used Yammer.com, a Web-based collaboration technology, which was not approved or monitored as required by VA policy. Further, we found that it had vulnerable security features, recurring website malfunctions, and users engaged in a misuse of time and resources. Although One VA Technical Reference Model (TRM) approved, with constraints, the installation of Yammer's Notifier, a Windows desktop application, use of the Yammer social network was not VA-approved for employee use. Further, it was not only promoted by VA employees, but it was used and showcased in June 2013 by Mr. Stephen W. Warren, former Executive in Charge of Information Technology (IT) and Chief Information Officer (CIO), for an open chat forum, as well as in a June 2014 CIO Message reminding employees to comply with VA Directive 6515 when using Yammer, giving the false impression that VA approved the use of Yammer.com. (Mr. Warren previously told us that he was VA's CIO from March 2013 to March 2015; however, the OIT website reflected that he held that position up until early July 2015.)

We also found that the Yammer website did not have an administrator or system set in place to ensure removal of former VA or contractor employees and the relatively simple process to post to Yammer not only made VA vulnerable from user uploading, on purpose or accidentally, personally identifiable information (PII), protected health information (PHI), or VA sensitive information, of which any current or former employee remaining active on the site would have access. We found Yammer users violated VA policy when they downloaded and shared files, videos, and images, risking malware or viruses spreading quickly from the site. We further found that Yammer regularly spammed and excessively emailed users, as well as VA employees who had no interest in joining the site, and users were unable to remove the *Online Now* instant messaging feature, resulting in every user violating VA policy simply by logging onto the site. We found numerous user posts that were non-VA related, unprofessional, or had disparaging

content that reflected a broad misuse of time and resources. Moreover, the continuous data streams, instant messaging, video, audio, large files and attachments, and other uploaded non-VA content to the site may cause congestion, delay, or disruption of service and degrade the performance of VA's network.

Introduction

The VA Office of Inspector General (OIG) Administrative Investigations Division investigated whether VA employees used Yammer.com, an unapproved Web-based collaboration technology. To assess this, we interviewed Mr. William Cerniuk, Veterans Health Administration (VHA) Technology Director; Mr. (b) (6), (b) (7), VA contractor employee; Ms. (b) (6), (b) (7)(C), VA contractor employee, and other VA employees. We also reviewed VA Yammer posts, emails, Yammer and Microsoft open source information, other relevant documents, as well as Federal laws and regulations and VA policy.

Background

VA Directive 6515, dated June 28, 2011, identifies social networks as a Web-based collaboration tool or technology and that when properly used can significantly enhance VA's mission effectiveness. It states:

> VA endorses the secure use of Web-based collaboration tools to enhance communication, collaboration, information exchange, and citizen engagement; streamline processes; and foster productivity improvements, when it is done in accordance with applicable laws, regulations, and policies. Web-based collaboration tools enable widely dispersed facilities and VA staffs to more effectively collaborate and share information to achieve productivity, efficiency, and innovation.

Yammer, as defined by *PC Magazine Encyclopedia*, is "a private social networking service for businesses." It further described Yammer as a tool launched in late 2008 that "lets companies create their own social network site for employees as well as customers. Private groups within the company can also be organized" and the site can be accessed via a "desktop application, the Web, e-mail, instant and text messaging, as well as smartphones." In June 2012, a news article, *Microsoft to Acquire Yammer*, announced Microsoft acquired Yammer and that Yammer joined the Microsoft Office Division.

OIT's presentation, *Social Media 101, An Introduction to OIT's Upcoming Social Media Strategy*, stated that VA's Yammer network was created in 2008 by an IT Project Manager who "realized and appreciated the value of being able to connect with colleagues in an informal format without clogging email inboxes." The presentation

stated that "Yammer enables real-time collaboration and discussion for workforce teams," describing the Yammer platform similar to Facebook and Twitter but "designed for professional use," such as "company communication, team collaboration, and knowledge exchange." The presentation answered the question, "Why should I use Yammer?" with "Use Yammer at work to foster team collaboration, empower employees, drive business agility, and socialize [our] intranets. Use Yammer to provide group review of documents, take meeting notes, and discuss solutions to existing problems."

Mr. Cerniuk told us that he was one of the first three VA employees to sign up for access to Yammer and described it as a "social media site which is semi-private, allowing the ability for VA employees who have VA email addresses, contractor [or] permanent, to have discussions that do not involve PII or PHI." Mr. (b) (6), (b) (7)(C) told us that his staff began using Yammer in early 2012 as an "organizational approach" to disseminate product development messaging. He said that Yammer was an "enterprise social media network" that was "essentially, for lack of a better definition, Facebook for your company." Ms. (b) (6), (b) (7)(C) said that "while the SharePoint internet is a series of websites and portals, the Yammer system is more like Facebook where you go in and voluntarily set up your own profile. You can put your picture on it, and it is more of a forum where you can post things, share interesting articles, discuss hot topics. It is like a physical watercooler."

In June 2013, Mr. Warren, a registered VA Yammer user since May 2011, hosted a question and answer forum on Yammer. He began the session stating, "Before I take questions, I want to stress that I am committed to strengthening transparency as we work together to become the best and most secure IT product and service delivery organization..." Over 170 VA Yammer users "followed" his chat. By August 3, 2015, Yammer reflected 25,171 VA email addresses registered with active members and another 25,609 VA email addresses registered on Yammer which were not yet activated.

Results

Issue: Whether VA Employees Improperly Used Yammer.com

Federal regulations state that employees shall use official time in an honest effort to perform official duties. 5 CFR § 2635.705.

VA policy states that the Secretary designated the Assistant Secretary for Information and Technology as VA's CIO, the senior agency official responsible for VA's IT programs. It also states that the CIO is responsible for the effective use of VA's internet, intranet, and other IT resources, and for agency-wide directives, and policies governing the use and implementation of internet/intranet and other IT resources. Further, it states that the CIO shall ensure that secure access is provided to all approved Web-based collaboration tools, including websites operated by non-VA entities, provide oversight and guidance related to Web-based collaboration tools…work with the Assistant Secretary of Human

Resources and Administration to develop and establish standard operating procedures for disabling access for individuals who establish, maintain, or are responsible for posting content to eternally-hosted Web-based collaboration tools when those individual transfer or are terminated from these duties. VA Directive 6515, Paragraph 3b.

VA policy also states that to establish an official VA social media account, the petitioning office, employee, or organization must demonstrate: 1) a business case for the site; 2) adequate resources are available to establish and maintain the site; 3) and that the organization's previously established website is also kept up-to-date and meets VA quality standards. The Office of Public and Intergovernmental Affairs (OPIA) is the final approving authority for all VA social media sites, except those of the Office of the Inspector General, which is exempt from this oversight and control per the Inspector General Act. However, OPIA may delegate approval or disapproval to administration communications offices after coordinating with those offices to ensure the maintenance of content standards. Id., at Paragraph 2(h). VA policy also states that the Assistant Secretary for OPIA shall review and approve or disapprove requests by VA organizations to launch official social media presences, have the authority to disapprove any outward-facing content on official VA blogs and social media sites which do not meet accepted standards of quality, conduct periodic review of social media sites to ensure alignment with VA messaging and priorities, and certify that those sites may continue to operate after audits are concluded. Id., at Paragraph 3(e).

VA policy states that Web-based Collaboration Service Coordinators are responsible for ensuring all social media websites for which they are responsible remain on topic and do not contain: PII, excessive or vulgar language, personal attacks of any kind, offensive comments that target or disparage any protected class, spam, subjects clearly off topic, language advocating illegal activity, promotions of particular services or products or political organizations, copyrights of trademarks not owned by the person posting them, VA sensitive data, or anything that clearly violates VA policy. In addition, they must ensure that all VA blogs under their responsibility contain the "Social Networking Disclaimer" found in Appendix A of VA Directive 6515. Id., at Paragraph 3(m)

Moreover, VA policy states that Web-based collaboration tools established for official VA use must be approved, authorized, monitored, and moderated. As the content owners, each administration, staff office, program office, and facility is responsible for monitoring and maintaining all posted Web content and assuring that the information is accurate and current. Id., at Paragraph 2(g). A Web Page Privacy Policy (or link to the approved statement) must also be posted on the introductory page in accordance with VA Handbook 6502.3. Further, all VA social media pages or sites must contain the "Social Network Disclaimer" found in Appendix A of VA Directive 6515. If the notice is not on the main page, the homepage must include a prominent link to the notice. In these cases, the marking must clearly identify the notice as "Privacy and Security – Legal Notice." Id., at Paragraph 2(o). Furthermore, it states that Web-based collaboration tools must

also meet standard records retention and e-discovery requirements as mandated by law and that Under Secretaries, Assistant Secretaries, and Key Officials shall provide proper records management retention in accordance with applicable Freedom of Information Act (FOIA) requirements, e-discovery litigation holds, and Records Control Schedule (RCS), or if the records are unscheduled under RCS, ensure they are retained until scheduled by the Archivist of the United States. Id., at Paragraph 2x and Paragraph 3h(4).

VA Pamphlet 005-12-6, issued by VA OIT, states that "you should never download or share files, videos, or images to a VA computer through social networking sites. Even if the information seems to be from a trusted contact, it could be carrying malware [defined as any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems] or viruses [defined as a malware program that, when executed, replicates by inserting copies of itself into other computer programs, data, files, or the boot sector of the hard drive] in the coding. Malware or malicious software can spread quickly on a social network site, infecting your computer and spreading to your contacts." It also states that "when you participate on a VA social media site as a VA employee, you represent the Department, and you are personally accountable for the content you post. If you are officially authorized to speak on behalf of VA, you will use your VA social media account to share posts that represent VA's official position. However, if you want to post personal views on a VA social media site, you must do so using your personal social media account as a private individual."

VA policy states that VA personnel utilizing Web-based collaboration technologies, wherever possible, must use the VA intranet for the conduct of VA business. VA personnel using external technologies for collaboration activities must ensure that this use complies with law guidance and VA policy. VA Directive 6515, Paragraph 3(p). Further, it states that access to Web-based collaboration tools that access, disseminate, or process sensitive information must be restricted to those VA personnel who have a need to know for the performance of their professional duties. Id., at Paragraph 2t. It further states that VA personnel and organizations must exercise sound judgment when utilizing Web-based collaboration tools. The use of these tools must promote the mission, goals, and objectives of VA and be consistent with applicable laws, regulations, and policy, as well as prudent operational, security, and privacy considerations. Id., at Paragraph 2d.

VA policy further states that when interacting on weblogs (blogs, wikis, social networks, virtual worlds and social media), VA personnel must: never comment on VA mission-related legal matters unless they are VA's official spokesperson for the matter, and have General Counsel and management approval to do so; be professional at all times when posting to VA-related social media, and use their best judgment when interacting on social media about matters related to VA's mission; in their capacities as VA representatives, post only information about which they have actual knowledge. They must never comment or provide information on any matter about which they do not have actual, up-to-date knowledge; never use profanity, make libelous statements, or use

privately created works without the express, written permission of the author; only post and use content in accordance with applicable ethics, intellectual property, records, and privacy laws, regulations, and policies; use Government Office Equipment including IT in accordance with VA Directive 6001, Limited Personal Use of Government Equipment including Information Technology; and use only VA-approved instant messaging services. Id., at Paragraph 3p.

VA policy states that employees are expected to conduct themselves professionally in the workplace and are required under the Standards of Conduct to refrain from using Government office equipment for activities that are inappropriate. Misuse or inappropriate personal use of Government office equipment includes any personal use that could cause congestion, delay, or disruption of service to any Government system or equipment. For example, continuous data streams, video, sound, or other large file attachments can degrade the performance of the network. VA Directive 6001.

In a June 13, 2014, CIO Message, Mr. Warren stated:

> For many of us, social media has become a part of our lives. Some VA employees also use social media websites to communicate with Veterans and other stakeholders. Unfortunately, social media websites can serve as a vehicle for identity theft and other cybercrimes…Whether you operate a VA social media account to communicate with the public, or simply interact with co-workers via Yammer or blogs like OI&T360, you must comply with VA Directive 6515….

Yammer was Not Approved or Monitored

On April 29, 2015, One-VA TRM approved Yammer's Notifier software, released in September 2008 and May 2011, for installation on VA-issued equipment, with permission from the employee's supervisor, Information Security Officer (ISO), or local OIT representative. The One-VA TRM website stated that downloaded software must always be scanned for viruses prior to installation to prevent adware or malware. Yammer's website reflected that their Notifier was a "desktop companion to the Yammer web experience that keeps you in the loop, even when you don't have Yammer open."

Mr. (b) (6), (b) (7)(C) told us that the VA Yammer network was "created" in 2008 when a VA IT project manager heard about Yammer and created an account, not realizing that she "was actually the first person on the network." He said that "if you're the first person from that email domain, Yammer automatically creates a Network…. Once she signed up for it, the network was created." Mr. Cerniuk told us that the first individual on VA Yammer registered using their @va.gov email domain, "so the first person signing up literally by time-wise created the network by the act of signing up." Mr. (b) (6), (b) (7)(C) said that the VA Yammer network continued to grow when the project manager's colleagues used and shared it. He said that "people then just continued to share and invite people to join…

and the network kind of snowballed and created itself organically." The VA Yammer users we contacted were unable to confirm whether or not the website was approved by OPIA or who was the responsible party to ensure it met the standards within VA policy and properly approved.

Ms. Megan Maloney, OPIA's Director of Digital Media Engagement, told us that OPIA had "not approved terms of service for the use of Yammer within the VA system" and that she had "no records" or "memory of any official approval" for Yammer. She said that "in order for [Yammer] to be an official VA social media channel, we need to have VA negotiated terms of service. We have negotiated nearly a dozen terms of service in the last 2 years. Yammer is not one of them."

Furthermore, no one could identify a Web-based Collaboration Service Coordinator for VA's use of Yammer. Mr. (b) (6), (b) (7)(C), (b) (6), (b) (7)(C), OPIA Digital Media Engagement, told us that they were unable to find who managed VA Yammer, and Mr. Cerniuk told him that he [Mr. Cerniuk] managed it. However, Mr. Cerniuk told us that there was not one individual "officially" monitoring or moderating the site, as administrative rights were not included in Yammer's basic network, VA's current form of service. Mr. (b) (6), (b) (7)(C) told us that because there was "no [one] person running the network necessarily" that "no one has…authority" to place a Web Page Privacy Policy on the introductory page or the "Social Network Disclaimer," as required by VA policy.

Mr. Cerniuk told us that Yammer's basic network "model is to have decentralized social administration" with no one individual holding administrative privileges. He said that it was a "free service until someone takes complete ownership of the service, at which point they're given administrative rights to the entirety of the data." Mr. (b) (6), (b) (7)(C) told us, "now it's kind of like a self-policing, everybody's job is to be responsible" and that in order for VA Yammer to have "network administrators who can monitor" the site and content, VA would have to forego the free basic network version and purchase a Yammer Enterprise Network model.

Yammer's basic network terms of use, something all VA Yammer users agreed to when they use or access Yammer, stated, "Your Organization may decide to assume control over the Services by purchasing a Yammer Enterprise Network…In such a case, an Admin assumes and has full control over accounts associated with their Organization's domain email address and may delete the Account or Content of one or more users." Yammer's administrative guide further detailed that network-wide admin privileges were only included in a purchased Yammer Enterprise Network. Administrative privileges include the ability to: configure network settings, features, and applications; set network design, including logo and color scheme; create usage policy and require all users to accept it; see all unlisted Groups; delete any messages; post announcements; remove or block any user; manage user account activity; bulk update users; read messages in any Private Group; and configure security settings.

Mr. Cerniuk told us that just prior to the June 2012 Microsoft buyout of Yammer, he was involved in an informal evaluation of the costs and benefits of VA paying for the Yammer service. He said that he found that the paid version cost "$30 a seat per year" and that "it wasn't worth paying" for the fee-based enhancements of Yammer "over the free…The free was good enough." He said that "up to that point, self-moderating was an honest to goodness success," but the "$30 a head would give us the ability to manage our network directly and own it as an administrator…a VA employee given administrator rights, given the ability to, for example, add people, kick them out, change account information, change look-up pages, do a lot of things including connect Yammer to our VA authentication system if we so [choose]." Yammer Enterprise Social Network Pricing and Plans reflected that pricing, as of March 2013, for the Yammer Enterprise Standalone decreased from $15 per user per month to starting at $3 per user per month. Mr. Cerniuk told us that depending "on our Microsoft license now, we may have the ability to get a significant discount on Yammer."

Yammer's Vulnerable Security Features and Recurring Website Malfunctions

Mr. Cerniuk told us, and Yammer's terms of use reflected, that an individual on Yammer's basic network owned the contents of what they uploaded or shared on the site, but that if the owner of the organizational domain purchased a Yammer Enterprise Network, the organization then owned the content instead of the individual user. Yammer's admin guide stated that "messages posted within your Home Network are owned by your company and cannot be shared externally without permission," if they are on the Yammer Enterprise Network. Yammer's terms of service stated that you are only able to join an organization's Yammer basic network if you join using the email address provided by that organization. Mr. (b) (6), (b) (7)(C) told us that Yammer was "restricted to your email domain. So, only people with the same email domain can join. So, there's a VA network. The only people that can join it are people with @va.gov email."

Mr. Cerniuk told us that when he initially researched the cost and benefit of VA paying for Yammer's service, the cost was too high for the benefit; however, he said that VA "should negotiate with the Yammer folks and sign up for the full monty…because if nothing else, it would be good to have the VA have import-export capability, own the data, and be able to actually moderate conversations" as necessary. He also said that it would be good to be able to manage the "uploads and downloads…my concern is that somebody is going to post a PowerPoint up there that has PII or PHI." He said that he did his best to examine uploads "but obviously that's not part of my overall job. So it's very difficult for me to take that on as a full responsibility." He told us that "if anything, the OIG would be most concerned with…floating of actual Word documents and things like that. So if we could monitor that, that would be worth the price." Mr. Cerniuk told us that the standards contained in VA Pamphlet 005-12-6, requiring VA employees to never download or share files, videos, or images to a VA computer through social networking sites, are "not being followed anywhere."

Beyond the concern of a VA Yammer user posting PII or PHI, we found posts that exemplify how a user could potentially share VA sensitive information, posing security concerns for VA. On April 18, 2013, a user, who was also an information security officer (ISO), posted "Figured out how to copy the [Personal Identity Verification (PIV) Public Key Infrastructure (PKI)] Certificate to windows if a card is lost or not working[;] all the email encrypted with the certificate can still be accessed without the card." He attached a visual document showing computer screenshots with his post titled, "Installing your PIV PKI certificates to your PC." Although we found that the process he detailed did not successfully export PIV PKI certificates, he posted a process that he believed would directly circumvent VA's IT security.

Further exemplifying the potential to share VA sensitive information, we found a user replied to another user's post, "Please DELETE the .pdf with the IP address IMMEDIATELY! IP addresses are VA protected information and may NEVER be posted in a public place – even if only VA public. If necessary to put in an email the email should be encrypted. This is a security violation. Thank you!" We found the .pdf file attached to the posting was deleted within 24 hours.

Another user posted, "This is the most difficult site I have ever been on. I received an email that my password had been changed and if I didn't change it to contact customer support. Followed the link and could find no way to communicate with customer support. This is ridiculous. Who knows who accessed my account and changed the password. Yammer won't because I cannot contact them."

A VA Informatics and Computing Infrastructure Program Specialist posted to Yammer on June 18, 2013, that she "notice[d] that many former employees of the VA are still listed as members of VA Yammer groups" and asked if there was a "procedure for deleting members from our Yammer groups once they've been removed from the Active Directory?" Several users responded, and one provided information on how to remove a user. The following is a partial continuation of their conversation:

> User 1: I just did the delete for a friend who left last year. I should have done it last year!! It's "deactivated" her…
>
> User 2: So, if someone leaves the VA and nobody sends a message to have that account suspended, can the former employee still participate in the VA Yammer groups?
>
> User 1: Yes. They theoretically could. They just need to sign into yammer. Keep in mind, yammer is not behind the firewall, so anyone with a connection to the internet can gain access. Yep, even Hackers. Hmm, now that makes me curious about security.

> User 2: me too…Also, just discovered that there's a limit of suspending 5 accounts per month unless you upgrade.
>
> User 3: Also as long as we[']re talking security of account. Who's to stop someone from selecting another person[']s account and marking them for removal? That is a good reason why we need applications tied to your VA account that way once someone is gone and the account is disabled they would lose access by design.

Mr. Cerniuk told us that Yammer does not have a centralized administrator, "which means that at any given point in time you or I or anyone else in Yammer can hit a button next to my name that says, 'This person is no longer in the network,' and it will disable my login and ask me to confirm my email that I am, in fact, part of the network. If I don't confirm that on email… it proves that I'm no longer part of it and I'm taken out. Now, this is not done by any rigor of any sort. No one is assigned this duty of going through and digging out who belongs. So people will be able to log into Yammer after they leave the VA if their account isn't disabled either by themself or otherwise."

Mr. (b) (6), (b) (7)(C) told us that as long as Yammer was "being engaged as a free network" the responsibility in reporting the former VA employee and contractor accounts "lies with every employee." Mr. (b) (6), (b) (7)(C) said that "the reason that some [former VA employees and contractors] exist on the network is based on the fact that that's kind of a self-policing model. If you're on an enterprise network, you're able to see, and have an administrator that can actually delete old people that are no longer VA employees or contractors." A Microsoft help article, *How to remove a former employee from the Yammer network,* stated that only administrators in a Yammer Enterprise Network could "delete users immediately" and "decide to keep or delete the user's messages."

We also found instances in which Yammer improperly emailed VA employees or spammed—defined as irrelevant or inappropriate messages sent on the Internet to a large number of recipients—VA Yammer users. For example, on May 5, 2014, a user posted:

> I received 8 consecutive emails between 10:31-11:14 AM. The first one was a welcome message but it was someone else's name. The second one was a welcome message with another person's name. Third one was confirming a password change. Fourth one was another welcome notice with yet another person'[s] name. Fifth message was another password change notice. Sixth one was a link to verify my email address (I have not clicked on it). Seventh message is directed to one of the other three persons welcomed earlier. Eighth message is a "hate to see you go…you will be permanently prevented from receiving Yammer notifications[.]" WHAT IS GOING ON?

Another user replied, "Me too, someone named Edwin. I changed my password."

The following is a portion of a conversation on March 15, 2012:

> User 1: My husband has received several invitations to join Yammer from people he does not know. When he contacts them they say they did not invite him, and do not know how they received an invitation in their name. I know there isn't a system administrator for VA Yammer. Is there some way to find out how these unwanted invites are being generated?
>
> User 2: I can tell you one of the ways it happens. User error. I can say this, because I did it by accident. I invited a whole slew of people who'd been invited before. After I did it, a couple of people did the same thing. I got lots of nasty "I don't want to do this, take me off the list" messages in much less friendly terms than what I just wrote….
>
> User 1: He did join back when I did but at that time the option to receive a weekly digest wasn't functional. He got tired of his mailbox filling up so he deleted his account…

On March 18, 2014, another user posted:

> URGENT – need help with Yammer spamming my colleagues – Good morning. Yammer is spamming (yamming?) my colleagues, and I need help! When I joined Yammer via my company (U.S. Department of Veterans Affairs) a couple weeks ago, I was asked for my colleagues' names. It said that would help "customize my experience." Well, what's happening is that those people are receiving multiple emails asking them to join Yammer. The list of people being yammed includes my boss's boss and other people at that level. These people are way above me in the chain of command, and I need this to stop ASAP. I tried to find a list of those people inside my Yammer account, but no dice. I've tweeted @YammerSupport and plan to call as soon as it's business hours on the west coast. Please – is there anything that can be done? This is embarrassing, and if it continues, it's going to get very unpleasant for me around here.

The following are posts in May 2014 by two VA Yammer users that further exemplify the regularity of Yammer website malfunctions:

> User 1: Think maybe Yammer hiccupped this afternoon. It showed me with 279 notifications! None were new. Was I the only "lucky" one?
>
> User 2: I received a notice twice this morning that someone has joined Yammer. The next email I receive is "This email confirms that your password for the VA network on Yammer has been successfully changed.

> If you did not take this action, please contact Yammer support immediately. Thank you, The Yammer team." This message occurred after the announcement of the persons joining. Is the password change message referring to them because I have not changed my Yammer password?

Additionally, on May 7, 2014, Yammer posted that a VA Yammer user "#joined the VA network. Take a moment to welcome [Name]." The following is a partial continuation of the conversation:

> User 1: Glad you made it. I got a response from Yammer saying your email was not valid.
>
> User 2: I received three Yammer invitations from you. Which address was not valid?
>
> User 2: Did you see my Yammer response? I'm not sure why you got the email message.
>
> User 2: I'm not a tech guy, but this posting when responding to email feature looks dangerous to me!...I'm willing to give it a try.

On November 24, 2014, Yammer "invited" a VA OIG Administrative Investigator to join the VA Yammer network, although the investigator never visited or provided their email address to Yammer. The investigator received an email with the subject line "VA Learning University has invited you to the VA network." The body of the email stated, "I've added you to Yammer…We're using our VA network on Yammer to talk about team projects and get updates from across the company. We need your input and ideas. Join us on the network." The email provided a link to "Accept Invitation." We were unable to determine if this unsolicited email was generated by Yammer or by a potential hacker—defined as a person who secretly gets access to a computer system in order to get information—masquerading as a trustworthy entity.

VA employees are required to use only approved forms if instant messaging services; however, we found the Yammer instant messaging feature, *Online Now*, automatically loads when the user accesses the VA Yammer internet site. A Microsoft support article, *Information about the Online Now feature in Yammer*, stated "*Online Now* gives Yammer users a new, faster way to start discussions with their coworkers. Regardless of where you are in Yammer, you can connect to *Online Now* in the lower-right corner of the screen." We found we were unable to manually disable the feature and the Microsoft article stated that Yammer users could not change their presence on the *Online Now* feature to "Busy" or "Away" or any other customization to show that the VA Yammer user did not wish to be contacted using the instant messaging tool.

Misuse of Time and Resources by VA Yammer Users

On June 12, 2015, a VA OIG Administrative Investigator received a Yammer email that reflected Yammer had 61 new VA members that day, and cited the following posts:

> User 1: I'm beginning to suspect the reason for a lot of VA backlogs is the constant need to create new and even more complex passwords, seemingly every five minutes.
>
> User 2: Now VOIP phones require a 12 character password and change every 90 days. Was there a risk assessment done that determined there is a high threat of someone logging into my phone?
>
> User 3: When in doubt let's go to the Extremes!...The mentality is Shoot First, Aim later…

Mr. (b) (6), (b) (7)(C) told us that Yammer is used for "a number of enterprise functions, mostly as kind of an internal watercooler, discussing, connecting with colleagues remotely." Ms. (b) (6), (b) (7)(C) said that "the best way to describe" VA Yammer is "while the SharePoint internet is a series of websites and portals, the Yammer system is more like Facebook where you go in and voluntarily set up your own profile. You can put your picture on it. And it is more of a forum where you can post things, share interesting articles, discuss hot topics. It is like a physical watercooler."

Mr. (b) (6), (b) (7)(C) told us that historically "there have been some issues with Yammer" and that "some people are somewhat unprofessional on that service." He said that OPIA "tried to find out who was actually managing the VA account in the past due to some unwise postings" but was "unsuccessful" since the VA Yammer is a Yammer basic network, not Yammer Enterprise, and cannot have an administrator.

We found some users frequently posted to VA Yammer or commented on other posts. One user, an individual who frequently posted news articles, posted a TribLIVE.com article, *How VA red-flags veterans,* on June 30, 2014. There were 54 response posts on the article by a number of VA Yammer users over a span of 3 days. The following are excerpts from user comments on the article:

> User 1: Every time you post this crap, I am going to call you out on it.
>
> User 2: Hearing from you [Name], someone personally involved with the decision process was rewarding. If further questions or comments arise I look forward to reading your input rather than hearing nonsense from the friends and family pulpit…

User 1: Just to be clear – my wife works for the Directors Office Chief of Staff – I work for OI&T, which doesn't have a direct reporting chain of command with the hospital. Two completely different organizations.

User 2: [Name], [it] further depresses me to read your comments, even though we find them [quite] funny. It's obvious you have taken advantage of the friends and family hiring program the VA endorses just like [so] many others do, but enjoy the benefits, because many Veterans only wished they had 10% of your fun time. Best wishes.

User 3: [Name], seriously. Why do you have to be so mean-spirited? Maybe you don't have any friends and family that […] want to work in the VA, maybe with you. I don't understand why you work for the VA and meanwhile, all you do is post negative postings about the VA and the federal government in general. We all know the federal government is not perfect and pretty much like most companies and corporations in America. You just sound like a disgruntled employee who skates by his displeasure of working with VA by posting media articles that state exactly how you feel about the federal government. You're ashamed of working for the fed gov? QUIT. Find another job that won't threaten your "integrity." I'm still trying to find a way to block your postings that show up on my feed so don't bother replying to this because I'm not going to answer. You're a bitter bitter person and it just makes me sad for you. I'm done reading anything with your name on it.

User 4: Wow, [Name]! Is free speech banned on Yammer? And talk about mean spirited and name calling… Just Wow!

User 5: [Name], I have read many of your postings and agree with some of them. The article you cited was appropriate to post here, and the subsequent comments have pointed out that, as in all organizations, well-meaning policy does not always preclude bad behavior.

However, your 'friends and family' comments need to stop. And not just because both my wife and I work for the University of Utah here at the Salt Lake City VA. You are insinuating impropriety and attacking personal integrity where you have NO EVIDENCE. I suspect that is not your true intent. Engaging in social media discourse does not mean framing everything with unicorns and cute kittens, but it does require civility. Please honor that.

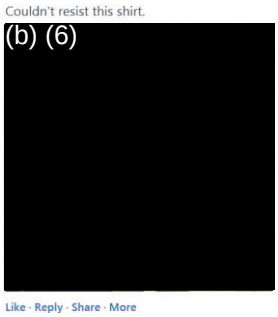
User 3: I'm sorry, [Name] but this is a VA Yammer (an internal communications network within the VA), not Facebook. It's frustrating to have my feed bombarded with the bias-based newsmedia (most, not all)

> about our employer. I won't do it again; as soon as I can get these postings to not show up on my feed. I'm all into free speech; but not when he's being mean to people who reply to his postings. I'm not trying to be rude but, in my opinion, he needed to be called out on his passive-aggressive replies. It's not cool. That is all.

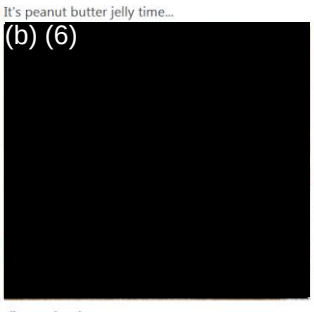
We found many examples of users misusing official time and posting non-VA related photos on Yammer. We did not examine their time and attendance records, but the posts were during normal duty hours. On April 24, 2013, a user posted "Who else likes [Name's] coat today? I sure do! [Name]?" The post generated 29 responses by users over a span of 17 days.

Below are further examples of non-VA related postings:

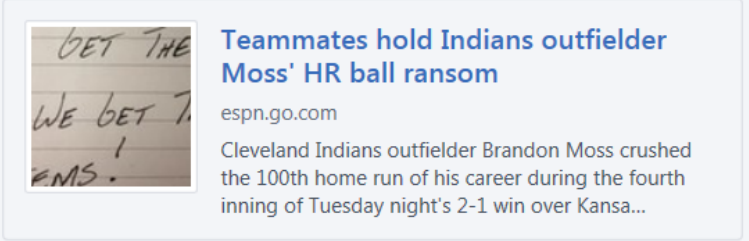
- On Friday, May 15, 2015, at 3:31 p.m., a VA employee posted this t-shirt photo.



- On Tuesday, May 26, 2015, at 7:09 a.m., a VA employee posted this sock photo.



- On Thursday, June 4, 2015, at 8:05 a.m., a VA physician posted comments and this link to a sports article.



- On Friday, June 5, 2015, at 2:20 p.m., a VA employee posted comments and this video link.

Yammer Groups

We found VA Yammer users were able to join and follow "Groups." A Yammer article described Groups as "flexible, collaborative workspace for teams to get work done wherever, whenever…." The article stated that a Yammer user could "set up a Group in seconds for any team, project, or interest. Share project updates, collaborate on a campaign launch, or organize your next team event with a Group. Groups can be public or private." We were unable to view private Group postings; however, in public Group postings, we found numerous jokes, cartoons, political comments, video feeds, and internet links to non-VA related articles, online videos, and webpages.

The following are examples of Groups created by users on the VA Yammer Network:

- *GEEK Jokes* – 584 members as of June 2015 and a description, "Know something that only a geek will laugh at? Post it here and share the relief. PS Try to keep it clean…" We found the group included posts such as a photo article titled *10 Tricks to Appear Smart in Meetings*; an illustrated photograph titled *What your style of beer says about you*, with 16 beers and descriptions; and an illustrated picture of a group eating lunch with text depicting a conversation, "Isn't weed just for reggae, Like, if you want it to sound good?" "No, my brother uses it for something called Phish, which is kind of like circus music, and Raffi, but bad."

- *Swap Meet* – 267 members as of June 2015 and a group description, "A place for VA'ers to buy, sell, trade or give away personal stuff amongst each other." We found the group included posts by users offering to sell or purchase numerous items, such as a book collection, an iPod touch, baseball cards, an executive desk, and similar personal conversations.

- *VA Young Professionals* – 224 members as of June 2015 and a description of "bringing together those of us that are young and youngish for networking. And the occasional happy hour."

- *Fifty Shades of Craig* – 19 members as of June 2015 and included posts containing images of a man's head superimposed on various nonsensical non-VA images.

Conclusion

We substantiated that OIT and other VA employees improperly used Yammer.com, a Web-based collaboration technology. Although the desktop application software, Yammer Notifier, was approved with constraints, for use, the Yammer social network was not. Even though it was not authorized for use, or monitored, it quickly became widely used by VA employees, without ever going through the appropriate approval process or first meeting the standards set forth in VA Directive 6515. We found that VA Yammer did not have the required Web-based Collaboration Service Coordinator, resulting in no one individual ensuring that the social media site did not contain improper posts, such as VA sensitive data, inappropriate content, or a misuse of official VA time and/or resources.

We further found that VA Yammer was not only used and first promoted by OIT personnel, but used and showcased by Mr. Warren, VA's then CIO, who was responsible for providing oversight and guidance, as well as ensuring that, once approved, secure access was provided to it. Instead, he not only used the unapproved VA Yammer site to hold an open chat forum, but in a CIO message reminding users to comply with VA policy when using the unapproved site, giving the false impression that Yammer was approved for VA employees to use. Moreover, VA employees used Yammer's basic network model, which did not permit VA to have an administrator or administrator rights and VA did not own the content the users posted to the site. With no site administrator, these records may not be kept as required by law for record retention.

We further found that Yammer had vulnerable security features and recurring website malfunctions. There were no restrictions for accessing this Web-based collaboration tool, other than having a @va.gov email address when signing up for access. After signing up, any user could access, disseminate, or process sensitive information, which should be restricted to VA personnel with an official need to know, and there was an ability to privatize Group pages so that VA officials could not see the content of their posts. Further, there was no administrator or system set in place to ensure former VA employees and VA contractor employees no longer had access or that VA users did not, accidentally or on purpose, upload PII, PHI, or VA sensitive data. Further, certain activities made VA vulnerable to malware or viruses, which could spread quickly on a social media site, because of a false sense of security that VA approved the use of Yammer. Thus, about 50,000 VA email addresses were registered on Yammer, and half of those were active VA Yammer members. It was perceived as a trusted Web-based collaboration tool, used by trusted sources, and used frequently to download, upload, or share files. However, VA guidance states that employees should never download or share files, videos, or images to a VA computer through social networking sites, as they

may carry malware or viruses which could spread quickly, infecting computers and contacts.

We found that, in mass, VA Yammer users not only violated VA policy and guidance when they posted comments, uploaded, downloaded, shared files, and linked videos on the site, but just by logging into Yammer activated the *Online Now* instant messaging feature, which could not be disabled. Moreover, we found several posts that contained VA sensitive data and numerous posts in which users posted or uploaded unprofessional, non-VA related personal, and/or disparaging content that showed a broad actual and potential misuse of time and resources by VA Yammer users. VA Yammer was not only an unapproved Web-based collaboration tool, it was a misuse of VA time and resources when VA employees used it, due to it not being properly approved. Further, the frequent use of Yammer, to include the instant messaging tool, could cause congestion, delay, or disruption of service and degrade the performance of VA's network.

Recommendation 1. We recommend that the VA Chief of Staff confer with the Offices OIT, OPIA, and General Counsel (OGC) to ensure that VA Yammer is formally evaluated, approved, and/or disapproved for VA use. If approved, ensure it meets all Federal laws and regulations, as well as VA policy and guidance. If disapproved, ensure that all VA employees cannot access it from VA-issued equipment or VA's network.

Recommendation 2. We recommend that the VA Chief of Staff confer with the Offices of Human Resources (OHR), Accountability Review (OAR), and OGC to determine the appropriate administrative action to take, if any, against accountable OIT and OPIA officials, as well as other VA and contractor employees involved in this particular matter.

Recommendation 3. We recommend that the VA Chief of Staff ensure that all VA employees are made fully aware of which Web-based collaboration technologies VA has approved for their use and which are prohibited.

Comments

The VA Chief of Staff was responsive, and his comments are in Appendix A. We will follow up to ensure that recommendations are fully implemented.

QUENTIN G. AUCOIN
Assistant Inspector General for
Investigations

Appendix A

VA Chief of Staff Comments

Department of Veterans Affairs **Memorandum**

Date: July 28, 2015

From: Chief of Staff (00A)

Subject: OIG Draft Report, Administrative Investigation: Improper Use of Web-based Collaboration Technology, Office of Information and Technology (OIG Case No. 2013-03054-IQ-0155)

To: Director, Administrative Investigations Division, VA Office of Inspector General (51Q)

1. I have reviewed the draft report and concur with the report's recommendations. Attached is the Department's corrective action plan for Recommendations 1-3.

2. Thank you for the opportunity to review the draft report. If you have any questions, please contact Laverne Council, Assistant Secretary for Information and Technology and Chief Information Officer, at (202) 461-6911; or Josh Taylor, Deputy Assistant Secretary for Public Affairs, at (202) 461-7216.

VA Chief of Staff's Comments to Office of Inspector General's Report

The following VA Chief of Staff's comments are submitted in response to the recommendations in the Office of Inspector General's Report:

OIG Recommendation(s)

Recommendation 1. We recommend that the VA Chief of Staff confer with the Offices OIT, OPIA, and General Counsel (OGC) to ensure that VA Yammer is formally evaluated, approved, and/or disapproved for VA use. If approved, ensure it meets all Federal laws and regulations, as well as VA policy and guidance. If disapproved, ensure that VA employees cannot access it from VA-issued equipment.

Comments: OIT will work in collaboration with OPIA and OGC to determine whether and within what parameters VA Yammer should be approved for VA use. OIT will also work in collaboration with OGC to clarify Departmental policy with respect to VA employees' limited personal use of Federal government office equipment, including information technology, for non-Federal government purposes.

Target date for completion: October 1, 2015.

Recommendation 2. We recommend that the VA Chief of Staff confer with the Offices of Human Resources (OHR), Accountability Review (OAR), and OGC to determine the appropriate administrative action to take, if any, against accountable OIT and OPIA officials, as well as other VA and contractor employees involved in this particular matter.

Comments: The Department will review all available evidence with respect to inappropriate use of VA Yammer by specific VA employees to determine appropriate administrative actions, including but not limited to administrative investigations, disciplinary actions, and/or training.

Target date for completion: October 1, 2015.

Recommendation 3. We recommend that the VA Chief of Staff ensure that all VA employees are made fully aware of which Web-based collaboration technologies VA has approved for their use and which are prohibited.

Comments: The Department will explore options for clarifying the parameters of appropriate use of Web-based collaboration technologies through updated policy issuances, training, and/or other communication strategies.

Target date for completion: October 1, 2015.

Appendix B

OIG Contact and Staff Acknowledgments

OIG Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Acknowledgments	Leanne Shelly

Appendix C

Report Distribution

VA Distribution

Deputy Secretary (001)
Chief of Staff (00A)
Executive Secretariat (001B)

To Report suspected Wrongdoing in VA Programs and Operations:

Telephone: 1-800-488-8244

E-Mail: VAOIGHotline@va.gov

(Hotline Information: www.va.gov/oig/hotline)