UNITED STATES POSTAL SERVICE

STATEMENT OF
RANDY S. MISKANIC
VICE PRESIDENT, SECURE DIGITAL SOLUTIONS
U.S. POSTAL SERVICE
BEFORE THE
SUBCOMMITTEE ON FEDERAL WORKFORCE,
U.S. POSTAL SERVICE AND THE CENSUS
UNITED STATES HOUSE OF REPRESENTATIVES

NOVEMBER 19, 2014

Good morning, Chairman Farenthold, Ranking Member Lynch, and members of the Subcommittee. Thank you, Chairman Farenthold for calling this hearing on Data Security at the Postal Service. My name is Randy S. Miskanic and I serve as Secure Digital Solutions Vice President of the United States Postal Service. In this role, I lead the Postal Service's digital product development initiatives with the goal of aligning our innovation strategy with customer demand for secure digital communications and experiences. I am also a Postal Inspector, and previously served as the Deputy Chief Inspector of the United States Postal Inspection Service (USPIS). The Postal Service and I are firmly committed to extending the trusted and secure aspects of the Postal Service brand into our digital innovations and future product offerings.

As the USPIS Deputy Chief Inspector, I led the USPIS's strategic approach to the prevention and investigation of identity theft and fraud offenses in the physical and digital arenas. During that time, I advanced the capability of the USPIS to conduct cyber investigations, respond to malware and network attacks and analyze digital evidence. I also guided the USPIS's efforts to build a robust cyber response and investigative capability through partnerships with the Carnegie Mellon University's Computer Emergency Response Team Coordination Center (CERT-CC) and other federal government and private sector partners.

With the discovery of the recent cyber intrusion into some of the Postal Service's information systems—an incident that has received broad media coverage—our Mass Data Compromise Response Plan (MDCRP) was invoked to ensure the appropriate level of technical, investigative and communications response. Given my prior experience in Secure Digital Solutions and in federal law enforcement, the Postmaster General appointed me to the role of Incident Commander to direct MDCRP activities.

I want to assure this subcommittee that protecting the privacy of customer and employee information is a priority for the Postal Service. The cyber security intrusion investigation, led by the Federal Bureau of Investigation (FBI) and joined by other federal and postal law enforcement and investigatory agencies, is ongoing.

The intrusion is limited in scope and nearly all operations of the Postal Service are functioning normally. Sadly, this incident is similar to a growing number of attacks reported by many other federal government entities and U.S. corporations. We are not aware of any evidence that potentially compromised customer or employee information has been used to engage in any malicious activity, and we are working with impacted individuals to mitigate potential misuse of such information.

Threat Assessment and Response Timeline

From the time we became aware of the potential threat to Postal Service information systems, our guiding principles were to protect our network from additional harm, to ensure our employee and customer data was secure, and to initiate an investigation that would not be detected by our adversary.

As our investigation of this incident progressed, it became apparent that the intrusion was very sophisticated and had been developed specifically to exploit the Postal Service computing environment. In fact, over the course of the investigation, we learned of the dynamic tactics employed by the adversary to evade detection by most commercial information security tools.

As the scale and scope of the intrusion became evident, we greatly escalated our response. One of our biggest challenges was maintaining secrecy regarding the remediation of several of our infected systems. Therefore, we worked closely with the U.S. Computer Emergency Readiness Team (US-CERT), the FBI and other forensic experts to develop a strategy for protecting our network.

Following is a high-level timeline of how the Postal Service learned of, investigated, mitigated and communicated the threat. I believe that you will find this timeline clearly reflects how—upon discovery that some of our information systems had been intruded—the Postal Service responded quickly and collaboratively, following the advice and guidance of federal and private sector cyber security experts.

Initial Discovery and Investigation

On September 11, 2014, the U.S. Postal Service Office of Inspector General (USPS OIG) reported that they received information from the US-CERT regarding four Postal Service servers that were sending unauthorized communication outside of the organization, indicating that these systems may have been compromised. Limited details were provided by US-CERT at that time.

During the period of September 12 through September 16, the USPS OIG alerted the Postal Service's Corporate Information Security Officer (CISO) of the suspicious network activity. The CISO was advised that the investigation should remain confidential. Furthermore, the USPS OIG provided the CISO with an operational security warning advising that actions taken without coordination are likely to adversely impact the Postal Service's overall security posture. The guidance document instructed the CISO to take no action – including further investigative

activity, scanning, re-imaging, resetting account passwords, taking systems offline or searching IP addresses.

The guidance provided by the USPS OIG was consistent with subsequent direction received from US-CERT and other agencies who have been engaged with these types of actors. The Postal Service's Chief Information Officer (CIO) was also subsequently notified of the threat during this period, and received the same security and operational warnings.

From September 16 through September 19, USPS OIG agents, Postal Inspectors, and members of the CISO team met daily to develop the steps necessary to properly investigate the suspected unauthorized network activity. Members of the investigative team performed forensic imaging and installed monitoring devices on servers suspected of being compromised. At this point all that was known is that four servers were sending unauthorized communications.

On September 19, the Postal Service CIO reported the suspicious network activity to the Postmaster General (PMG). The PMG was also advised at that time that the cyber intrusion investigation was ongoing and that only the USPS OIG and USPIS should take action to mitigate the threat and that any premature action could further endanger the network. Subsequently, information regarding this incident remained highly confidential and restricted to only individuals directly involved with the investigation.

During the period of September 19 through October 2, USPS OIG agents and Postal Inspectors configured and installed the technical architecture and tools necessary to identify any impacted servers and workstations on the Postal Service network. These investigative actions resulted in the identification of three Postal Service user accounts and an additional 29 servers with indicators of compromise. Due to the broadening scope of compromise and resulting forensic analysis requirements, data was submitted to the U.S. Department of Defense Cyber Crime Center for forensic analysis.

On October 7, following five days of investigation that revealed suspicious remote communications emanating from several of the compromised machines, the USPS OIG and USPIS team learned that a large data file had been copied and removed from the Postal Service network. This file, however, was encrypted, limiting the ability of the investigative team to identify the data contained within. It was suspected that the file was copied to another server outside of the USPS network that was being controlled by an adversary. Extensive investigative efforts continued over the following days in an attempt to identify the content and location of the removed file.

On the evening of October 10, the CIO informed the PMG of the confirmed data exfiltration. The following day, the USPS OIG held a briefing with senior postal leadership to advise them of the incident and to develop a further course of action. It was decided that private sector experts specializing in computer intrusion and incident response would be sought to engage in the investigation and support mitigation planning.

From October 11 through October 15, USPS OIG agents and Postal Inspectors continued to monitor network traffic for additional compromised servers and workstations. During this period, USPS OIG agents conducted a forensic examination of the server containing the encrypted files. The ongoing investigation revealed that the adversary may have accessed and copied a Postal Service Human Resources file containing employee personally identifiable information (PII).

Mass Data Compromise Response Plan Invoked

On October 16, the PMG and postal leadership were advised by USPS OIG investigators of the suspected contents of the exfiltrated file. The investigators cautioned, however, that further extensive and complex forensic analysis was necessary to determine if the file actually contained PII.

The Postal Service CIO concurrently invoked the MDCRP—declaring that the critical incident would be managed through a formal Incident Command structure. As the appointed Incident Commander, I subsequently formed teams to handle various aspects of the plan—specifically, Technical Branch, Communications Branch and Investigative Branch teams.

The Technical Branch was charged with developing the remediation and mitigation strategy, along with assisting in the overall ongoing investigation. The Postal Service Information Technology (IT) Team was assembled under this Branch and immediately began working with US-CERT to determine more detailed information about the threat. This Branch also began consulting with Carnegie Mellon University's CERT-Coordination Center (CERT-CC), Microsoft Corporation, and other commercial firms specializing in computer intrusion incident response, network monitoring, and remediation strategies to assess the adversary's capabilities and tactics. These partners were also involved with evaluating the protection of critical Postal Service cyber assets.

The MDCRP Communications Branch was tasked with developing a strategy to communicate the ongoing incident to necessary stakeholders, and to develop a comprehensive internal and external communications plan. A critical component that was discussed extensively and thoughtfully planned, was content and timing of employee messaging in the event that the suspected loss of PII data was confirmed. Strategic business partner and public notification were also critical communications elements that required extensive planning efforts.

The MDCRP Investigative Branch was bolstered by additional resources and assigned specific actions to identify the scope of compromise, along with the impact on Postal Service data systems. A strategic and tactical support request was submitted to the FBI. In response, the FBI provided cyber security intrusion experts, communication support for stakeholder and public outreach, and introductions to executive contacts within other intelligence agencies.

On October 17, the FBI Cyber Unit provided a Top Secret/Sensitive Compartmented Information briefing to the Postal Service Incident Command leadership and advised that the adversary was

very sophisticated and that implementing mitigation activities or communicating the threat to employees or the public at that point could result in the threat being further embedded into the Postal Service network. The FBI also reemphasized the need to exercise a high level of operational security during the management of this critical incident.

During the following week, USPS OIG agents and Postal Inspectors continued to obtain forensic images and established network monitoring across the entire Postal Service organization.

Administration and Congressional Notification

On October 20, the Incident Command staff provided a classified briefing to the White House Cyber Security Director and National Security Council staff. The White House Cyber Security Director was instrumental in aligning the Postal Service with the appropriate Federal resources to assist with all facets of managing the critical incident.

On October 22, the Deputy Postmaster General, U.S. Postal Service Inspector General, Chief Postal Inspector and I conducted separate classified briefings for House Oversight and Government Reform Committee and Senate Homeland Security and Governmental Affairs Committee staffs. The Committee staffs were informed of the current status of critical incident activities, the proposed plan to implement remediation within the Postal Service network, and the suspected compromise of employee PII data.

Also on October 22, USPS OIG agents learned that forensically recovered employee data appeared to originate from the Postal Service Human Resources Shared Service Center, however, contents of the encrypted files were still not known.

Communications Planning Intensifies

On October 23, the MDCRP Communications Branch team began working with select internal Postal Service department representatives to develop action plans for communicating with stakeholders during a hypothetical incident in which employee PII was accessed by an external entity. While it was still unknown at that time if employee PII had in fact been taken, all department representatives were required to plan for this scenario during a series of confidential meetings. As a result of the follow-up exercises, pertinent areas of focus, necessary tasks, and services required to assist potential victims were identified.

A significant challenge in developing communications that would provide the necessary information and details regarding available assistance, was that the contents of the compromised data was unknown for much of the time between discovery and announcement. As the technical analysis of the intrusion identified the scope of the breach, we tailored messaging to ensure all affected victims would be provided with the information necessary to assist in protecting them from the consequences of any illegal use of the compromised data.

Timing of public communication was also a serious concern. From the technical perspective, experts within the Postal Service and from supporting agencies provided prudent warnings that short-term remediation efforts would be seriously compromised if the threat actor became aware that the intrusion had been discovered. If provided advance warning of network actions intended to expel and block the intruder from the Postal Service network, the adversary could take bolder steps to further infiltrate or sabotage systems. This valid threat of additional potential damage to the Postal Service and victims was deemed sufficient basis to delay notification and public announcement until after short-term remediation was accomplished.

Another concern focused on the needs of the victims of this network intrusion. In similar data breaches within other organizations, potential victims attempted to reach support services, such as credit monitoring, before those services were in place and ready to assist. We sought to avoid any additional frustration for our employees and affected customers, and we worked with our credit monitoring vendor to ensure victims would be able to access services in a timely manner.

An inability to effectively answer employee, customer, and business partner questions regarding the specific content and victims of the compromised data created yet another concern. Prematurely announcing the intrusions before these important facts were discovered would have undoubtedly led to a great deal of frustration and confusion.

US-CERT Engagement Increases

On October 23, US-CERT officials also briefed postal leadership and Incident Command staff about the type of adversary likely responsible for the intrusion. The officials also reinforced FBI guidance regarding operational security practices, cautioning against public notice and mitigation actions being taken too soon.

The US-CERT Director provided critical strategic advice regarding the scope, phases and duration of activities associated with the deployment of the remediation plan. Additionally, the Director cautioned that the Postal Service was moving very aggressively and an improperly resourced plan could alert the adversary, which could then open the Postal Service network to deeper penetration and make eliminating unauthorized access more difficult.

From October 26 through October 28, the forensically recovered employee PII data from the compromised server was reconstructed and shared with the Postal Service Chief Human Resources Officer (CHRO). The investigative team subsequently confirmed through detailed forensic mapping and analysis that the recovered Postal Service employee PII was indeed compromised by the adversary. Review of additional forensic evidence indicated that files were extracted to a server outside of the Postal Service network, albeit the investigative team still did not know what, if any, files actually were stolen.

On October 31, the investigative team identified a database backup file on a compromised server, which was determined to be related to an application used for receiving, processing and

managing customer service requests. The database backup file was located on a compromised server that was determined to have 2.9 million customer complaints. The compromised customer data was limited to name, address, phone and email address information provided in the course of each customer complaint.

Data Compromise Confirmed and Remediation Plan Activated

On November 4, the investigative team—with the assistance of US-CERT—confirmed that the Postal Service employee PII data was copied and stolen from the Postal Service network. The scope of the compromised data included, names, dates of birth, social security numbers, addresses, beginning and end dates of employment, emergency contact and other information. The following day, the Postal Service received mitigation recommendations from US-CERT to successfully evict the adversary from the Postal Service network.

On November 7, the Postal Service CIO organization activated a remediation plan developed with US-CERT guidance and supported by external cyber security experts. Implementing remediation plan elements required initiation of an information systems network brownout period, which limited communications between the Postal Service network and the Internet.

Also on November 7, the Deputy Postmaster General, Chief Postal Inspector and I also conducted a joint briefing for House Oversight and Government Reform Committee and Senate Homeland Security and Governmental Affairs Committee staffs regarding the timing of our remediation plans and employee and public notifications.

During the November 8 – November 9 brownout period, virtual private network (VPN) connections were blocked and remote network access was denied. Sending and receiving email messages between Postal Service email accounts was allowed during the brownout, however, sending and receiving emails messages between postal accounts and non-postal accounts was blocked. The brownout did not affect mail collection, processing, and delivery operations. In addition, retail, usps.com, and employee and customer-facing applications functioned normally during this period.

The new network security safeguards put into place over this two-day period included removing workstation administrator rights and enhancing network monitoring. We also upgraded and segmented Administrative Domain Controllers, removed compromised systems and accounts, and implemented two-factor authentication for administrative accounts.

To further reduce the likelihood of phishing or spear-phishing emails—common and increasingly sophisticated ways of compromising computer users and systems—impacting the Postal Service network, access to personal email sites such as Gmail or Yahoo was, and continues to be, blocked. In addition, direct database access is now only enabled to technology support staff and a number of business applications have been retired. These safeguards will continue to be reviewed and enhanced over the coming months in order to increase our overall security posture.

Comprehensive Communications Plan Activated

With the confirmation that employee PII had actually been compromised, and completion of initial remediation efforts, the Postal Service quickly activated its comprehensive communications plan developed for this incident.

The PMG recorded a video to be used in conjunction with other messaging for the purpose of informing employees of the intrusion and remediation activities. Postal managers were provided prepared materials and instructed on how employee communications materials should be disseminated. In addition to the PMG video, prepared materials included hardcopy versions of mandatory employee stand-up talks, anticipated questions and answers, and talking points for communicating with customers. These materials were also posted to the Postal Service's intranet site. In addition, messaging on the cyber intrusion was included in the daily electronic newsletter delivered via email to all employees with computer access, and notices were posted on employee bulletin boards.

Key postal stakeholders, including Union and Management Association national presidents, strategic business partners, including mailing industry leaders, and heads of key federal agencies were personally contacted and informed of the security breach. The Administration, House and Senate Leadership and Congressional Oversight Committee members were also informed that public messaging of the cyber intrusion was beginning. Electronic newsletters delivered information to subscribing customers. Customer information about the intrusion, including a fact sheet and anticipated questions and answers, were also posted on usps.com and other postal customer-facing websites

Customer Impacts of Cyber Intrusion

At this time, we do not believe that Postal Service transactional revenue systems in Post Offices, as well as on usps.com where customers pay for services with credit and debit cards, were affected by this incident. There is no evidence that any customer credit card information from retail or online purchases, change of address or other services was compromised. Postal Service operations were not impacted by the breach – Post Offices are functioning normally and mail and packages are being delivered as usual.

As noted earlier in my testimony, the intrusion did compromise data submitted by customers who contacted the Postal Service Customer Care Center with an inquiry via telephone or e-mail. For customers who provided such information between January 1, 2014, and August 16, 2014, this data consists of names, addresses, telephone numbers, email addresses and other information. The Postal Service does not believe that these potentially affected customers need to take any action as a result of this incident. While we are aware of no evidence that would suggest that credit monitoring is needed at this time, we are continuing to investigate and will of course provide such monitoring if it is deemed appropriate.

Employee Impacts of Cyber Intrusion

The investigation indicates that all 800,000 plus Postal Service career and non-career employees nationwide, including those working for the Postal Regulatory Commission, the Office of Inspector General and the U.S. Postal Inspection Service, have been affected by the breach. No beneficiary information was compromised, and the incident did not affect Postal Credit Unions or Thrift Savings Plan accounts. Compromised files may also have included PII for employees who left the organization anytime from May 2012 to the present. We are additionally aware of a possible compromise of injury compensation claims data that we are still investigating.

The Postal Service is making credit monitoring service available to all employees, as well as those who left the organization since May 2012, at no charge for one year. Last week, letters were sent to employees advising them of the compromised PII data and provided a unique activation code to enroll in the service within 90 days of the date of the letter. All employees are encouraged to take advantage of this service.

While we are not aware of any evidence that any of the compromised employee information has been used to engage in any malicious activity, the credit monitoring service is being offered out of an abundance of caution. Postal Service forensic investigators are conducting a thorough review of the affected databases and if the ongoing investigation determines that any additional employee information has been compromised, employees will be notified. Postal employees, like everyone else, are advised to keep vigilant for incidents of fraud and identity theft by regularly reviewing account statements and monitoring credit reports.

Next Steps

The privacy and security of data entrusted to the Postal Service is of the utmost importance. Our entire leadership team is committed to taking the steps necessary to prevent a cyber security intrusion from happening again.

During the activation of our remediation plan, Carnegie Mellon's CERT-CC performed a vulnerability assessment on systems that were compromised. The team evaluated both processes and technical security controls. The assessment included scanning and penetration testing of select human resource systems, review of vulnerability scans for select systems, interviews with system owners, and review of general security policies related to authentication, system hardening, and perimeter defenses.

CERT-CC found that the Postal Service has solid policies for information security; however, various business units do not always follow these policies. It also found that critical systems could be protected by better segregation from the general IT user systems. Starting with security measures that we put in place as soon as we confirmed that employee PII was compromised, we are continuing to institute numerous additional measures designed to improve the security of our information systems. One such future change includes requiring employees

to complete two-factor authentication to access individual user accounts and some applications. Additionally, we plan to request assistance from CERT-CC to conduct a full-scope vulnerability and penetration test of our network.

Going forward, the Postal Service will also increase our collaboration with government agency partners such as US-CERT and the National Cybersecurity and Communications Integration Center (NCCIC) to understand tactics used by cyber security adversaries, as well as other threats to national security. Additionally, we will continue to improve our security posture in line with US-CERT recommendations, which include increasing network monitoring, increasing network segmentation, improving user management controls, improving server security controls, thus improving our overall information security posture. These improvements will require the procurement of new hardware and information security services.

The Postal Inspection Service also will join the National Cyber Investigative Joint Task Force (NCIJTF). Membership in this task force will enhance the ability of the USPIS to proactively act upon intelligence information and learn more about evolving threats. In addition, Postal Inspectors will be better positioned to coordinate, integrate, and share information related to cyber threat investigations.

Conclusion

The Postal Service takes its responsibility to safeguard the personal information of our customers and employees very seriously. No company or organization connected to the Internet is immune from the type of malicious cyber activity that the Postal Service experienced. We take such threats seriously and regularly take action to protect our networks, our customers' data, and our employees' information.

As a result of this incident, we have significantly strengthened our systems against future cyber intrusions. We will continue taking all necessary steps to guard our systems from attacks and to ensure the safety and privacy of our employees and customers. Thank you, Mr. Chairman, for the opportunity to submit this testimony. I welcome any questions that you and the Committee members may have.

###