

U.S. OFFICE OF PERSONNEL MANAGEMENT

INFORMATION ABOUT OPM CYBERSERURITY INCIDENTS

- [What happened](#)
- [How you may be affected](#)
- [What you need to do](#)
- [What we are doing to help](#)

Check back weekly for the latest information.

What Happened

OPM recently discovered **two cyber-security incidents** that have impacted the data of Federal government employees, contractors, and others:

1. In April 2015, OPM discovered that the **personnel data of 4.2 million current and former Federal government employees had been stolen**. This means information such as full name, birth date, home address and Social Security Numbers were affected. This number has not changed since it was announced by OPM in early June and **you should have already received a notification if you were impacted**.
2. While investigating this incident, in early June 2015, OPM discovered that additional information had been compromised: including **background investigation records of current, former, and prospective Federal employees and contractors**. OPM and the interagency incident response team have concluded with high confidence that sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals, was stolen from the background investigation databases. This includes 19.7 million individuals that applied for a background investigation, and 1.8 million

non-applicants, primarily spouses or co-habitants of applicants. Some records also include findings from interviews conducted by background investigators and approximately 1.1 million include fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen. **Notifications for this incident have not yet begun.**

While background investigation records do contain some information regarding mental health and financial history provided by applicants and people contacted during the background investigation, there is no evidence that health, financial, payroll and retirement records of Federal personnel or those who have applied for a Federal job were impacted by this incident (for example, annuity rolls, retirement records, USA JOBS, Employee Express).

OPM and an interagency team from the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) have been investigating these incidents, and are working to put in place changes that will prevent similar thefts in the future.

How you may be affected

If you underwent a background investigation through OPM in 2000 or afterwards (which occurs through the submission of forms [SF-86 \(PDF file\)](#), [SF-85 \(PDF file\)](#), or [SF-85P \(PDF file\)](#) for either a new investigation or a reinvestigation), it is highly likely that you are impacted by the incident involving background investigations. If you underwent a background investigation prior to 2000, you still may be impacted, but it is less likely.

Learn more about who was impacted and the protections we are working to put into place.

- Current and former Federal government employees
 - If you are a current or former Federal government employee,

including members of the U.S. military, you may have been impacted by the incident affecting **background investigation records**. You may also have been impacted by the separate incident involving **personnel data**.

- Types of information involved in the **background investigation records** incident that may have been impacted:
 - Social Security Numbers
 - Residency and educational history
 - Employment history
 - Information about immediate family and personal and business acquaintances
 - Health, criminal and financial history that would have been part of your background investigation

Some records could also include:

- Findings from interviews conducted by background investigators
- Fingerprints.
- Usernames and passwords used to fill out your forms.

Some records also include findings from interviews conducted by background investigators and approximately 1.1 million include fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen.

If you may have used your e-QIP (the online system used to process forms) password for other accounts or services, you should change your passwords for those accounts immediately and not reuse any passwords that you used in the e-QIP system.

- Types of information involved in **personnel data** incident include:
 - Name
 - Social Security number
 - Date and place of birth
 - Current and former addresses
 - Common personnel file information such as job assignments, training records, and benefit selection decisions

Protections available to you:

1. We have sent notifications to those affected by the incident involving personnel data. We are offering free identity theft monitoring and restoration services. If you were affected by this incident, you have been sent a notice that includes information about the free services available to you for 18 months. As part of this service, you are *automatically* enrolled in:
 - Full service identity restoration, which helps to repair your identity following fraudulent activity;
 - Identity theft insurance, which can help to reimburse you for certain expenses incurred if your identity is stolen.

Instructions on how to enroll in other services were included in your notification.

2. **For those affected by the background investigation incident**, we will be providing you with a similar suite of comprehensive services in the coming weeks. You will receive a notice in the mail providing details on the incident and the services available to you at no cost for at least three years such as:
 - Full service identity restoration support and victim

recovery assistance

- Identity theft insurance
- Identity monitoring for minor children
- Continuous credit monitoring
- Fraud monitoring services beyond credit files

This notification will also include detailed information that you can provide to other individuals you may have listed on your form. This information will explain the types of data that may have been included on the form, best practices they can exercise to protect themselves, and the resources publicly available to address questions or concerns.

Your department or agency may reach out with additional information specific to you.

- Current and former Federal contractors

- Current or former Federal contractors may have been impacted by the incident affecting **background investigation records**. We have no evidence to suggest that current or former Federal contractors were affected by the separate incident involving **personnel data**.

Types of information in the incident **involving background investigation records**:

- Social Security Numbers
- Residency and educational history
- Employment history
- Information about immediate family and personal and business acquaintances
- Health, criminal and financial history

Some records could also include:

- Findings from interviews conducted by background investigators
- Fingerprints.
- Usernames and passwords used to fill out your forms

Some records also include findings from interviews conducted by background investigators and approximately 1.1 million include fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen.

If you may have used your e-QIP (the online system used to process forms) password for other accounts or services, you should change your passwords for those accounts immediately and not reuse any passwords that you used in the e-QIP system.

Protections available to you:

For those affected by the background investigation incident, we will be providing you with a similar suite of comprehensive services in the coming weeks. You will receive a notice in the mail providing details on the incident and the services available to at no cost for at least three years you such as:

- Full service identity restoration support and victim recovery assistance
- Identity theft insurance
- Identity monitoring for minor children
- Continuous credit monitoring
- Fraud monitoring services beyond credit files

This notification will also include detailed information that you can provide to other individuals you may have listed on your form. This information will explain the types of data that may have been included on the form, best practices they can exercise to protect

themselves, and the resources publicly available to address questions or concerns.

- Job candidates for federal employment who were required to complete a background investigation
 - Candidates who were required to complete a background investigation form prior to employment may have been impacted by the incident affecting **background investigation records**. We have no evidence to suggest that job candidates were affected by the separate incident involving **personnel data**.

Types of information in background investigation incident that may have been impacted:

- Social Security Numbers
- Residency and educational history
- Employment history
- Information about immediate family and personal and business acquaintances
- Health, criminal and financial history

Some records could also include:

- Findings from interviews conducted by background investigators
- Fingerprints.
- Usernames and passwords used to fill out your forms

Some records also include findings from interviews conducted by background investigators and approximately 1.1 million include fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen.

Some records also include findings from interviews conducted by background investigators and approximately 1.1 million include fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen.

If you may have used your e-QIP (the online system used to process forms) password for other accounts or services, you should change your passwords for those accounts immediately and not reuse any passwords that you used in the e-QIP system.

Protections available to you:

For those affected by the background investigation incident, we will be providing you with a similar suite of comprehensive services in the coming weeks. You will receive a notice in the mail providing details on the incident and the services available to you at no cost for at least three years such as:

- Full service identity restoration support and victim recovery assistance
- Identity theft insurance
- Identity monitoring for minor children
- Continuous credit monitoring
- Fraud monitoring services beyond credit files

This notification will also include detailed information that you can provide to other individuals you may have listed on your form. This information will explain the types of data that may have been included on the form, best practices they can exercise to protect themselves, and the resources publicly available to address questions or concerns.

- Spouses and co-habitants of current and former Federal employees, contractors, and job candidates whose information was stolen

- Social security numbers of the spouses and co-habitants of applicants were stolen as a result of the background investigation record incident.

Protections available to you:

For those affected by the background investigation incident, we will be providing you with a similar suite of comprehensive services in the coming weeks. You will receive a notice in the mail providing details on the incident and the services available to you at no cost for at least three years such as:

- Full service identity restoration support and victim recovery assistance
 - Identity theft insurance
 - Identity monitoring for minor children
 - Continuous credit monitoring
 - Fraud monitoring services beyond credit files
- Immediate family, close contacts, and references of current and former Federal employees, contractors, and job candidates whose information was stolen
 - Beyond applicants and their spouses or co-habitants described above, you may be someone whose name, address, date of birth, or other similar information may have been listed on a background investigation form. In many cases, the information about these people is the same as what is generally available in public forums such as online directories or social media, and generally does not present the same level of risk of identity theft or other issues. While services will not be provided to you at no cost, there are a number of steps you can take to protect your identity.

What you can do

At this time, there is no information to suggest misuse of the information that was stolen from OPM's systems. We are continuing to investigate and monitor the situation. We will begin to notify people affected by the **background investigation incident** in the coming weeks. At that time, you will be auto-enrolled in some services and will need to take action to enroll in others.

In the meantime, here are steps you can take to protect your identity:

- Spot the warning signs of identity theft
 - Visit IdentityTheft.gov to learn how to set up protections:
 - Get a free credit report
 - Set up fraud alerts on your accounts
 - Protect your children/minors from identity theft
- Be aware of [phishing scams](#)
 - Phishing is when a fraudster impersonates a business or someone you trust in order to get your private information. Never click on links you don't trust and don't give out your personal information. Legitimate organizations never ask for your information through texts, pop-up messages, or email. Scammers may call and pretend to be from the government or a business to try to get you to give them sensitive information. If a caller asks for your information, call back using a number you know to be legitimate.
- Update your passwords
 - If the information in your background investigation forms could be used to guess your passwords or if you are using the same password that you did when you filled out your background investigation form, change them. Use complex passwords of 10-12 characters, combining letters, numbers, and special

characters. Don't use something that is easily guessable for someone who knows you or has information about you. Don't repeat passwords for several accounts.

- Get up to speed on computer security
 - Review and check up on your practices for safe, secure and responsible online activity. Onguardonline.gov lists helpful steps you can take to make sure your computer is as safe as possible.
- If you think your identity has been stolen
 - If you believe your information has been misused, there are several steps you should take.
 - If you are concerned that you are **experiencing identity theft**, visit identitytheft.gov. This site explains steps you can take to recover your identity.
 - If you are concerned about your **child's** identity being stolen, the Federal Trade Commission has [information and resources](#) to know what to look for and how to get help.
- Learn how to keep your information safe from exploitation
 - You can find information about the measures you can take to ensure the safety of your personal information from cyber criminals at the National Counterintelligence and Security Center (NCSC) at <http://www.ncsc.gov>.

What we're doing to help

- Supporting people who have been affected
 - We have sent notifications to those affected by the incident involving **personnel data**. We are offering free identity theft monitoring and restoration services. If you were affected by this

incident, you have been sent a notice that includes information about the free services available to you for 18 months. As part of this service, you are *automatically* enrolled in:

- Full service identity restoration, which helps to repair your identity following fraudulent activity;
- Identity theft insurance, which can help to reimburse you for certain expenses incurred if your identity is stolen.

Instructions on how to enroll in other services were included in your notification.

For those affected by the background investigation incident, we will be providing you with a suite of comprehensive services in the coming weeks. You will receive a notice in the mail providing details on the incident and the services available to you such as:

- Full service identity restoration support and victim recovery assistance
- Identity theft insurance
- Identity monitoring for minor children
- Continuous credit monitoring
- Fraud monitoring services beyond credit files

For those who have questions. In the coming weeks, a call center will be opened to respond to questions and provide more information. If you are affected, you will not be able to receive personalized information until notifications begin and the call center is opened. OPM recognizes that it is important to be able to provide individual assistance to those that have questions, and will work with its partners to establish this call center as quickly as possible.

Protecting all Federal employees. In the coming months, the Administration will work with Federal employee representatives

and other stakeholders to develop a proposal for the types of credit and identity theft monitoring services that should be provided to all Federal employees in the future – regardless of whether they have been affected by this incident – to ensure their personal information is always protected.

- Continuing to strengthen cyber defenses at OPM and across the Federal Government
 - OPM continues to take aggressive action to strengthen its broader cyber defenses and information technology (IT) systems, in partnership with experts from DoD, DHS, FBI and other interagency partners.

Outlined in the [Cybersecurity Action Report](#), OPM has identified 15 new steps to improve security and modernize its systems, including:

- Completing deployment of two-factor Strong Authentication for all users;
- Expanding continuous monitoring of its systems;
- Hiring a new cybersecurity advisor

Director Archuleta has also directed a comprehensive review of OPM's IT system security to identify and immediately address any other vulnerabilities that may exist, and assess OPM's data sharing and use policies.

The Federal government, led by the Office of Management and Budget, is taking aggressive actions to continually strengthen its cyber defenses, and all agencies are currently engaged in a 30-day cybersecurity sprint, whereby immediate steps are being taken to further protect information and assets and improve the resilience of Federal networks. OPM is fully engaged in this effort.

Finally and importantly, OPM will participate, along with our interagency Suitability and Security Performance Accountability Council partners, in a 90 day review of key questions related to information security, governance, policy, and other aspects of this the security and suitability determination process, to ensure that it is conducted in the most efficient, effective and secure manner possible.

Click here for more information about what the U.S. Government is doing to improve our cyber defenses, enhance our response capabilities, and upgrade our incident management tools.

We will be adding FAQs to the site. Please let us know if you have questions you'd like answered by emailing cybersecurity@opm.gov.

U.S. Office of Personnel Management

Actions to Strengthen Cybersecurity and Protect Critical IT Systems

June 2015

I. Introduction

The recent intrusions into U.S. Office of Personnel Management (OPM) systems that house personnel and background investigation data for Federal employees and other individuals have raised questions about the security of OPM data and the integrity of its Information Technology (IT) assets. Since Director Archuleta arrived at OPM, she has led the agency in taking significant strides to enhance cybersecurity and modernize its IT systems – strides that are in many ways forging new territory and laying groundwork for the rest of government. But recently discovered incidents have underscored the fact that there is clearly more that can and must be done. Government and non-government entities are under constant attack by evolving, advanced, and persistent threats and criminal actors. These adversaries are sophisticated, well-funded, and focused. For that reason, efforts to combat them and improve Federal IT and data security must be constantly improving as well.

The following report provides a summary of the actions OPM has taken, those that are currently underway, and those that are planned for the future in order to meet this challenge. Many of these actions are based on recommendations that have been provided by independent experts such as the agency's Inspector General (IG), the Government Accountability Office (GAO), and other Federal partners. In the coming weeks and months, the agency will continue to consult with Congress, the IG, independent experts inside and outside of government, and others to identify further actions to strengthen cybersecurity and protect its critical IT systems.

II. Prior and Ongoing Actions to Improve IT System Security

Upon Director Archuleta's arrival, OPM engaged in an end-to-end review of its IT systems and processes. Based on that review, the agency developed a *Strategic Plan for Information Technology* to guide its efforts to protect its legacy systems to the maximum extent possible as it replaced them with more modern and secure systems. This plan laid out a multi-phase strategy to bolster security through realignment of professional staff, adherence to relevant laws, policies and best practices, and investments in modern tools. As Director Archuleta stated upon publication:

“[The plan] provides a framework that is rooted in the use of human resources (HR) data throughout a lifecycle (“strategy to separation”), allowing for reuse of that data in our HR systems to support agile HR policies; establishes enabling successful practices and initiatives, and enterprise and business initiatives that define OPM's IT modernization efforts; and creates a flexible and sustainable Chief Information Officer (CIO) organization led by a strong senior executive with Federal experience in information technology, program management, and HR policy.”

One of the principal elements of the plan was information security – to ensure the agency protects the identity and privacy of citizens and employees by implementing and actively monitoring standard

security controls in IT systems that effectively protect the large volume of sensitive personal data collected and stored by OPM IT systems.

Under Director Archuleta's leadership, OPM has made good on that commitment by taking 23 concrete steps to improve information security:

Improving Security

1. **Implemented two factor Strong Authentication** for all privileged users, and increased the percentage of unprivileged users with two factor Strong Authentication. Requiring the utilization of a Personal Identity Verification (PIV) card or alternative form of multi-factor authentication can significantly reduce the risk of adversaries penetrating Federal networks and systems. OPM has been a leader for the Federal government in this area.
2. **Restricted remote access** for network administrators and restricted network administration functions that can be performed remotely.
3. **Reviewed all connections** to ensure that only legitimate business connections have access to the Internet.
4. **Deployed new hardware and software tools**, including 14 essential tools to secure the network. OPM continues to deploy additional security tools to improve its cybersecurity posture, including tools that mask and redact data.
5. **Deployed anti-malware software** across the environment to protect and prevent the deployment or execution of cybercrime tools that could compromise the agency's networks.
6. **Upgraded Security Assessment and Authorization** for multiple systems.
7. **Established a 24/7 Security Operations Center**, staffed by certified professionals, to monitor the network for security alerts.
8. **Implemented continuous monitoring** to enhance the ability to identify and respond, in real time or near real time, to cyber threats.
9. **Installed more firewalls** that allow the agency to filter network traffic.
10. **Centralized security management and accountability** into the Office of the CIO and staffed it with security professionals who are fully trained and dedicated to information security on a full-time basis.
11. **Conducted a comprehensive review** of IT security clauses in contracts to ensure that the appropriate oversight and protocols are in place.
12. **Developed a Risk Executive Function** to ensure risk mitigation at the organizational, business process, and information system levels, including development of Risk Executive Charter and Risk Registry Template.
13. **Mandated cybersecurity awareness training** for the entire workforce.

Leveraging Outside Expertise

14. **Collaborated with agency partners** such as the Office of Management and Budget (OMB) and the National Institute of Standards and Technology to share, learn and standardize best practices, and to ensure information security policies are rigorous and cost-effective based on a risk assessment methodology that considers both current and potential threats.

15. **Worked with the intelligence community** and other stakeholders to identify high value cyber targets within the OPM network where bulk PII data are present, and mitigate the vulnerabilities of those targets to the extent practicable.
16. **Worked with law enforcement and other agencies** to shore up existing security protocols, enhance the security of its systems and detect and thwart evolving and persistent threats.
17. **Bringing in management and technology expertise** by adding experts from around the Government to help manage its incident response , provide advice on further actions , and ensure that Congress and the public are kept fully up-to-date on ongoing efforts.
18. **Helping other agencies hire IT leaders** to ensure they can acquire the personnel needed to combat evolving cyber threats. This includes leveraging tools and flexibilities such as direct hiring, excepted service hiring flexibilities and critical pay authority to bring IT and cyber experts from the private sector into the Federal government quickly and efficiently.

Modernizing Systems

19. **Invested in network remediation and stabilization** to modernize OPM's IT footprint. From Fiscal Year 2014 to 2015, OPM nearly tripled its investment in the IT modernization effort, from \$31 million to \$87 million. The President's 2016 Budget calls for an additional \$21 million to further this effort. These funds would pay for maintenance of a sustained security operations center (SOC) to provide critical oversight of OPM's security posture and real-time 24/7 monitoring of network servers to detect and respond to malicious activity. Further, this funding includes support for stronger firewalls and storage devices for capturing security log information used for analysis in incident response
20. **Standardized operating systems.** In alignment with an IG recommendation OPM will continue standardizing operating systems and applications throughout the OPM environment, with the ultimate goal of implementing configuration baselines for all operating platforms in use by OPM. Once these baselines are in place, OPM will conduct routine compliance scans against them to identify any security vulnerabilities that may exist.

Accountability

21. **Strengthened oversight of contractors.** In alignment with recommendations made by the GAO, OPM is in the process of developing, documenting, and implementing enhanced oversight procedures for ensuring that a system test is fully executed for each contractor-operated system. These procedures will expand the policy for oversight of contractor systems currently in OPM's IT Security and Privacy Handbook.
22. **Tightened policies and practices for privileged users.** Consistent with guidance from OMB, OPM is reviewing the number of privileged users , and taking steps to minimize their numbers, limit functions that they can perform, limit the duration of time they can be logged in, limit the functions that can be performed remotely, and log all privileged user activity. This review –to be conducted by the CIO and the new cybersecurity advisor –will be completed and will provide recommendations to the Director by July 15.
23. **Improved Portfolio Management** by hiring a dedicated Level 3 IT portfolio manager, as recommended by the IG, in December 2014 to lead its IT transformation efforts and ensure that security and performance requirements are addressed across the enterprise.

These actions have put OPM in a much stronger and more secure posture than it was, when Director Archuleta assumed her role. OPM systems currently thwart the millions of intrusion attempts that target its networks every month.

Moreover, it was because of the very cybersecurity enhancements described above that OPM was able to detect the sophisticated malicious activity on its network responsible for the recent incidents described below.

III. New Actions to Bolster Security and Modernize IT Systems

The interagency incident response team has reviewed OPM's systems and concluded that there is no evidence that the intruder remains active on those systems. Yet simply because there is no evidence that this particular threat remains active does not mean that we can decrease our vigilance. And in fact, OPM is doing just the opposite.

As discussed above, OPM has already taken a number of aggressive steps over the past 18 months to increase its cybersecurity capabilities and modernize its critical IT systems. But there is clearly more that can and must be done to meet evolving cyber threats. With that in mind, OPM is taking the following **15 new actions**. Director Archuleta has directed that these actions be carried out with all due speed, as further steps to protect the critical assets and data OPM is entrusted with are of the utmost urgency.

Improving Security

1. **Completing deployment of two factor authentication** – While OPM has implemented two factor Strong Authentication (through the use of smart card log in) for all privileged users, it continues to implement this process for unprivileged users. As of the end of the second quarter of Fiscal Year 2015, nearly half of unprivileged users were using two factor authentication. Director Archuleta has directed that the agency accelerate its migration to full two factor authentication, and that this process be completed – with all users migrated to smart card log in – by August 1.
2. **Expanding continuous monitoring** – OPM is working with the Department of Homeland Security (DHS) to implement the Continuous Diagnostics and Mitigation program by March 2016. OPM will aggressively work with DHS to accelerate this schedule. OPM will also mandate continuous monitoring of contractor systems where feasible.
3. **Ensuring access to contractor systems** – OPM will establish requirements for future contracts, as appropriate, to ensure access to contractor systems in the event of an incident. This will ensure that OPM and law enforcement agencies can access data and conduct effective and immediate response in the case of any future cyber incidents. OPM will also consider whether any additional authorities from Congress are needed in order to enforce such access.
4. **Reviewing encryption of databases** – As Director Archuleta has stated, full encryption of the databases that were accessed in the recent incidents would not have been feasible, as many of OPM's systems would not have worked if they were encrypted. Moreover, encryption

would not have kept out these particular actors. That said, encryption can be a valuable tool in the agency's overall cybersecurity strategy, as emphasized by multiple members of Congress in recent hearings. Accordingly, Director Archuleta has directed a review of all agency databases to determine if there are any instances where encryption is possible but is not currently in place – and if any such instances are found, to proceed with encryption of the data. The Director has directed this review be completed by July 15.

Leveraging Outside Expertise

5. **Hiring a new cybersecurity advisor** – Director Archuleta will hire a leading cybersecurity expert from outside of government who will report directly to her. This cybersecurity advisor will work with OPM's CIO to manage ongoing response to the recent incidents, complete development of OPM's plan to mitigate future incidents, and assess whether long-term changes to OPM's IT architecture are needed to ensure that its assets are secure. OPM expects this individual to be serving the agency by August 1.
6. **Consulting with outside technology and cybersecurity experts** – To ensure that the agency is leveraging private sector best practices and expertise, Director Archuleta has reached out to Chief Information Security Officers at leading private sector companies that experience their own significant cybersecurity challenges. OPM will be holding a workshop with these experts in the coming weeks to help identify further steps the agency can take to protect its systems and information.
7. **Increasing consultation with the Inspector General** – As OPM has embarked on its IT modernization effort, it has received and addressed recommendations from the IG at multiple points. To ensure that this collaborative work continues, Director Archuleta will meet with the IG on a bi-weekly basis to receive regular advice and counsel

Modernizing Systems

8. **Migrating to a new IT environment** – OPM is incrementally engineering a modern network capable of significantly increased security controls. This new network infrastructure environment, known as the Shell, will improve the security of OPM infrastructure and IT systems. Once the Shell is implemented, OPM IT systems will be migrated into this new environment from the current legacy Local Area Network/Wide Area Network (LAN/WAN). This process will adhere to the OPM Systems Development Life Cycle, derived from Federal standards to manage OCIO Portfolios, Programs and Projects.
9. **Finalizing the scope of the migration process** – In alignment with recommendations of the Inspector General, OPM will complete an assessment of the scope of its IT modernization process before the end of the fiscal year. As part of this – and as recommended by the IG – OPM will assess the level of effort and estimated costs of the migration process. OPM will continue to track, document, and justify any changes should those estimated costs need to change.
10. **Evaluating all contracting options** – In alignment with another recommendation of the IG, as OPM considers the appropriate avenues for the Mitigation and Cleanup phases of the infrastructure improvement process, it will conduct a thorough analysis on the most reasonable and appropriate course of action, and explore all available contracting avenues

to determine the best option for the health of its modernization project and for the taxpayer.

11. **Calling on Congress for additional support** – In addition to the proposal put forth in the President’s Budget, OPM has conducted a review to identify areas where additional funding would help accelerate the process of improving its systems. In doing so, the agency is identifying recommended enhancements that would accelerate its overall modernization project plan. OPM will be providing further detail on these proposed enhancements to the House and Senate appropriations committees by June 26.

Accountability

12. **Senior leadership accountability** – Director Archuleta will initiate monthly reviews with the CIO and new cybersecurity advisor of the agency’s IT modernization and information security efforts to ensure continued progress and accountability.
13. **Establishing regular employee and contractor training** – As discussed above, OPM has already conducted cybersecurity awareness training for all of its employees. Given the recent incidents, OPM will be refreshing this training for all employees and contractors handling sensitive information on appropriate cyber hygiene and practices, to ensure that every individual is doing their part to protect the agency’s sensitive data. Going forward, this training will be required on a bi-annual basis.
14. **Documenting incident response procedures** – While no two cyber incidents are exactly the same, agencies should have in place clear protocols and plans of actions prepared in advance to manage incident response. OPM will document Standard Operating Procedures for how it will work with other Federal partners in the event of any future incidents. It will share these procedures with the IG to solicit feedback and advice.
15. **Ensuring compliance with the Federal Information Security Management Act (FISMA)** – As recommended by the IG, OPM will modify the performance standards of all OPM system owners to require and monitor FISMA compliance for each of the information systems under their purview.

IV. Conclusion

OPM stores more Personally Identifiable Information (PII) and other sensitive records than almost any other Federal agency. This is a tremendous trust placed in the agency by the millions of current and former Federal employees, and one that OPM must continually earn through constant vigilance.

The recent breaches of OPM data make clear that cybersecurity must remain a priority for all agencies, but especially OPM. As President Obama has said, “Both state and non-state actors are sending everything they’ve got at trying to breach these systems...And this problem is not going to go away. It is going to accelerate. And that means that we have to be as nimble, as aggressive, and as well-resourced as those who are trying to break into these systems.”

Over the past 18 months, OPM has taken aggressive steps to improve security protocols, set up continuous monitoring of its systems, establish a centralized Security Operations Center, and other measures. These steps have established a firm foundation on which OPM will continue a steadfast and unyielding effort to position the agency as a leader in Federal cybersecurity. And in fact, they led

directly to uncovering the recent incidents described in this report. Without the steps, malicious actors would like continue to be actively in its systems.

The persistent and continuing attacks by malicious actors make it clear OPM must remain vigilant. That is why Director Archuleta has directed the 15 new actions described above. OPM will carry out these actions without delay. In addition, OPM is calling on Congress to take swift action to assist in this effort by providing additional resources to modernize OPM's IT systems and ensure continued appropriate oversight of the agency and its contractors.

In a world of evolving threats, there is no such thing as "total cybersecurity." But the actions outlined above, and continued collaboration with Federal partners, Congress, and outside experts will ensure that OPM has all the tools it needs to safeguard its systems and protect the men and women that serve the Federal government.