Cybersecurity Resource Center

FREQUENTLY ASKED QUESTIONS

What is the U.S. Office of Personnel Management (OPM) doing to further strengthen its cybersecurity and review its processes?

In partnership with experts from the Department of Defense (DoD), Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), and other Federal agency partners, OPM continues to take action to strengthen its broader cyber defenses and information technology (IT) systems.

Over the past year, OPM has taken significant steps to enhance its cybersecurity posture and provide identity protection and credit monitoring services to individuals whose data was impacted in the 2015 cyber incidents.

Upon discovering the breach, and in the immediate aftermath, OPM, working with a team of Federal partners, took swift action to protect information and assets and strengthen the resilience of its networks. Steps taken included:

- Completing deployment of two-factor strong authentication for all users, which provides a strong barrier to OPM's networks from individuals who should not have access;
- Implementing a continuous monitoring program for all IT systems;
- Creating and hiring a cybersecurity advisor position that reports to the Director;
- Establishing an agency-wide centralized IT security workforce under a newly hired Chief Information Security Officer (CISO);
- Deploying new cybersecurity tools, including software that helps to prevent malicious programs and viruses on OPM's networks;
- Implementing a Data Loss Prevention System which automatically stops sensitive information, such as social security numbers, from leaving the network unless authorized; and
- Enhancing cybersecurity awareness training with emphasis on phishing emails and other user-based social engineering attacks.

Over the last year, in partnership with the Office of Management and Budget (OMB), Department of Homeland Security (DHS), and others, OPM has taken many steps to significantly strengthen its cybersecurity capabilities, many of which are part of the President's Cybersecurity National Action Plan.

OPM has established a close working relationship with DHS leveraging its current cybersecurity offerings. In particular:

- OPM is one of the first agencies to fully implement DHS' Continuous Diagnostics and Mitigation (CDM) program, and is targeted to complete deployment by the end of summer 2016. CDM will allow OPM to communicate with DHS more rapidly and effectively during any cybersecurity incident.
- OPM has also completed the implementation of the latest release of Einstein, Release 3a, which is a DHS IT defensive system that collects, detects, and prevents many cyber threats and potential cyber attacks before they can reach OPM's networks and users.

These DHS initiatives have set the stage for OPM to move to a Continuous Monitoring (CM) approach. CM will allow OPM to manage its systems and enhance their security. OPM has worked in close consultation with its Inspector General as it designs this working model.

OPM has made significant progress in its work to design and deploy other cybersecurity capabilities and tools. OPM successfully implemented the requirement of Personal Identity Verification (PIV) two-factor strong authentication to access the OPM network. OPM has also enabled PIV authentication for many of our applications, enhancing our overall system security. OPM has also reduced the number of individuals who have greater administrative level access and implemented stringent safeguards to prevent the exfiltration of sensitive information. Since the discovery of the cyber incidents, OPM also patched security vulnerabilities identified in the e-QIP system, and has plans to fully rebuild the application.

OPM centralized cybersecurity resources under a Chief Information Security Officer (CISO) and published policies empowering the CISO and CIO organization to take proactive steps in securing and controlling access to sensitive information. OPM has implemented an aggressive program to strengthen the IT infrastructure due to the CISO's leadership, support of the OPM organization, and its partnership with DHS.

Cybersecurity is more than the latest technology; it is also about people and processes. The CISO organization has helped successfully manage cybersecurity related incidents and enhancement of general cybersecurity awareness across the OPM organization.

Cybersecurity awareness has been integrated into many internal communication products such as the Director's Blog and Help Desk emailed communications. The effectiveness of OPM's increased awareness was demonstrated in a recent DHS phishing exercise where OPM showed significant improvement as compared to prior phishing exercises at OPM and the performance of other Federal agencies. OPM has also been working with DHS to ascertain how our efforts are working in real time.

In summary, working across organizations within OPM and with its interagency partners, OPM has enhanced the use of technology, development and deployment of cyber skills, and the implementation of new processes and controls to strengthen the security of OPM's networks.

Cybersecurity is complex and ever-evolving work. We will continue to work with OMB and Congress to wisely use the resources OPM has received to allow OPM to continue to adapt and strengthen its cybersecurity posture now, and into the future.