FPKIMA Newsletter

Summer 2021 | Volume 7, Issue 3

Federal PKI Management Authority
Enabling Trust

Inside This Issue

EO Improving Nation's Cybersecurity

On May 21, 2021, President Biden signed an Executive Order to improve the nation's cybersecurity and protect federal government networks. Executive Order 14028 makes a significant contribution toward modernizing cybersecurity defenses by protecting federal networks, improving information-sharing between the U.S. government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur. It is the first of many ambitious steps the Administration is taking to modernize national cyber defenses. However, the Colonial Pipeline incident is a reminder that federal action alone is not enough. Much of our domestic critical infrastructure is owned and operated by the private sector, and those private sector companies make their own determination regarding cybersecurity investments. We encourage private sector companies to follow the Federal government's lead and take ambitious measures to augment and align cybersecurity investments with the goal of minimizing future incidents.

Specifically, the Executive Order the President signed will:

Remove Barriers and Provide More Transparency to Information Sharing Between Government and the Private Sector

The EO includes several measures that remove communication barriers between government and industry with respect to threats and breaches. Often IT providers are hesitant or unable to voluntarily share information about a compromise. Other times providers are not able to because of contractual obligations; in other cases, providers simply may be hesitant to share information about their own security breaches. EO removal of contractual barriers and requirement that providers share breach information that could impact Government networks is necessary to enable more effective defenses of Federal departments, and to improve the Nation's cybersecurity.

Modernize and Implement Stronger Cybersecurity Standards in the Federal Government

Perhaps the most impactful component of the EO is a real timeline towards agency adoption of Zero Trust architecture. Most security protocols assume that if you have the credentials to access a certain network, you can be trusted to work in it. Simply put, Zero Trust replaces that assumption with multi-factor authentication and more expansive data encryption. Within 60, 90, and 180 days of the order being issued, agencies will be required to first, update their existing plans to adopt cloud technology. Then second, work with the Department of Homeland Security (DHS) and the General Services Administration (GSA) to review agency-specific cybersecurity requirements that currently exist as a matter of law, policy, or contract and recommend to the FAR Council standardized contract language for appropriate cybersecurity requirements.

Improve Software Supply Chain Security

The Executive Order will improve the security of software by establishing baseline security standards for development of software sold to the government, including requiring developers to maintain greater visibility into their software and making security data publicly available.

- Continued on next page

continued from page (1)

It stands up a concurrent public-private process to develop new and innovative approaches to secure software development and uses the power of Federal procurement to incentivize the market. Finally, it creates a pilot program to create an "energy star" type of label so the government – and the public at large – can quickly determine whether software was developed securely. Too much of our software, including critical software, is shipped with significant vulnerabilities that our adversaries exploit. This is a long-standing, well-known problem, but for too long we have kicked the can down the road. We need to use the purchasing power of the Federal Government to drive the market to build security into all software from the ground up.

Establish a Cybersecurity Safety Review Board

The Executive Order establishes a Cybersecurity Safety Review Board, co-chaired by government and private sector leads, that may convene following a significant cyber incident to analyze what happened and make concrete recommendations for improving cybersecurity. Too often organizations repeat the mistakes of the past and do not learn lessons from significant cyber incidents. When something goes wrong, the Administration and private sector need to ask the hard questions and make the necessary improvements. This board is modeled after the National Transportation Safety Board, which is used after airplane crashes and other incidents.

Create a Standard Playbook for Responding to Cyber Incidents

The Executive Order creates a standardized playbook and set of definitions for cyber incident response by federal departments and agencies. Organizations cannot wait until they are compromised to figure out how to respond to an attack. Recent incidents have shown that within the government the maturity level of response plans vary widely. The playbook will ensure all Federal agencies meet a certain threshold and are prepared to take uniform steps to identify and mitigate a threat. The playbook will also provide the private sector with a template for its response efforts.

A new endpoint detection and response system

Analysis of recent cyberattacks on government networks has shown that the deployment of baseline cybersecurity tools and processes has often been inconsistent or too slow. EO 14028 establishes a new, government-wide Endpoint Detection and Response (EDR) system that gives greater visibility into detecting malicious activity and empowers more efficient data sharing across government in the event of a cyberattack.

Event log requirements

Prior to this EO, responses to cyber-attacks varied greatly and lacked consistency. That inconsistency was found in processes as specific as event logging. EO 14028 mandates that agencies adopt a consistent event logging process that will allow investigators and analysts to detect and disrupt attacks, minimize damage in cases of successful breaches, and identify trends when looking at events across multiple incidents.

Trust Store Management

During the August 3rd FPKI Technical Working Group Trust Store Management was also covered in light of the recent FCPCAG2 root migration. The FPKI team is working toward defining the scope of the issue, and currently gathering information about potential tools for future adaptability and use for managing trust stores. In addition, the team is gathering information on products with trust stores that might require management (e.g., specific browsers, firewall and VPN products, in addition to trust stores at the OS level etc.). Please email fpki@gsa.gov with information about any products used with an internal trust store.

EO 14028 Critical Software

NIST just released Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028 to outline security measures intended to better protect the use of deployed EO-critical software in agencies' operational environments. You can read the full release here.

SP 800-204B Attribute-based Access Control for Microservices-based Applications using a Service Mesh

This document provides deployment guidance for building an authentication and authorization framework within the service mesh that meets these requirements: zero trust and ABAC.

NISTIR 8369 Status Report on the Second Round of the NIST Lightweight Cryptography Standardization Process

NIST initiated a public standardization process to select one or more Authenticated Encryption with Associated Data (AEAD) and hashing schemes suitable for constrained environments. The status report can be found here.

Where Can I Find More Information about the FPKIMA?

For more Information about the FPKIMA, go to https://www.idmanagement.gov/governance/ficam/#federal-public-key-infrastructure-management-authority or the FPKI Guide website at https://playbooks.idmanagement.gov/fpki/.

PKI in the Cloud

During the August 3rd FPKI Technical Working Group PKI in the cloud was discussed. Questions gathered from multiple entities were presented, and the need to document potential overlap and gaps between FedRAMP requirements and PKI requirements was discussed. Remote CA access was a hot topic in terms of compliance with PKI requirements. Additionally, the list of potential PKI cloud vendors was discussed with a recommendation to include all vendors with current FedRAMP cloud services.

A communications strategy was discussed, considering the following options: 1) Survey, 2) a single panel with multiple vendors, or 3) 1:1 engagement with vendors at a series of meetings. Additional research and analysis comparing the FedRAMP security controls with compliance audit requirements will be conducted.

NISTIR 8320A Hardware-Enabled Security: Container Platform Security Prototype

In today's cloud data centers and edge computing, attack surfaces have significantly increased, hacking has become industrialized, and most security control implementations are not coherent or consistent. The foundation of any data center or edge computing security strategy should be securing the platform on which data and workloads will be executed and accessed. The physical platform represents the first layer for any layered security approach and provides the initial protections to help ensure that higher-layer security controls can be trusted.

This report explains an approach based on hardware-enabled security techniques and technologies for safeguarding container deployments in multi-tenant cloud environments. It also describes a proof-of-concept implementation of the approach—a prototype—that is intended to be a blueprint or template for the general security community. Part of the Certificate Policy Working Group (CPWG) agenda will cover discussion on containers. To read NISTIR 8320A click here.

Migration to Post-Quantum Cryptography: Project Description Released

The National Cybersecurity Center of Excellence (NCCoE) has posted the final project description for the Migration to Post-Quantum Cryptography project. This effort complements the NIST post-quantum cryptography (PQC) standardization activities.

The NCCoE will solicit participation from industry to develop and demonstrate practices to ease migration from the current set of public-key cryptographic algorithms to replacement algorithms that are resistant to quantum computer-based attacks. These practices will take the form of white papers, playbooks, and demonstrable implementations for organizations. The audience for these practices is intended to include organizations that provide cryptographic standards and protocols, and enterprises that develop, acquire, implement, and service cryptographic products.

Federal PKI Working Group Updates

The **Certificate Policy Working Group (CPWG)** Audit and Archive Work team met throughout the quarter to make progress on potential changes to existing audit and archive policy requirements.

The FPKI Technical Working Group (TWG) 2021 Meeting Schedule
The most recent TWG was held on August 3rd where four topics were discussed. India Donald presented an update on Public Trust TLS. The group then touched on IPv6 in FPKI, PKI in the cloud and Trust Store Management.

Do you have a topic that you would like to be addressed during an upcoming TWG? Please send any topics or questions to fpki-help@gsa.gov.

Add these dates to your calendars and look for meeting specifics as it gets closer to the date of each meeting. Meetings will be held on a quarterly basis:
2021
1) November 2nd at 2:00 p.m. to 3:30 p.m. (times are subject to change)
2022
2) February 1st at 2:00 p.m. to 3:30 p.m. (times are subject to change)
3) May 3rd at 2:00 p.m. to 3:30 p.m. (times are subject to change)
4) August 2nd at 2:00 p.m. to 3:30 p.m. (times are subject to change)

Participation in Federal PKI working groups is limited to Federal employees, contractors, and invited guests.

Ask the FPKIMA

Can I be notified of new certificate issuances or other system notifications?

Yes! System notifications including; changes to Certificate Revocation List Distribution Points (CDP) and Online Certificate Status Protocol (OCSP) endpoints, new or retiring URIs, and signing or revoking a CA certificate are posted to the FPKI Guides System Notification page at https://playbooks.idmanagement.gov/fpki/notifications/.

You can subscribe to system notification and other issues by signing up for a GitHub account and watching the FPKI guide repository at https://github.com/GSA/ficam-playbooks.

Need Help?

Certificate doesn't validate? Unsure which certificate to use?

ASK THE FPKIMA

fpki-help@gsa.gov

Request for Topics

Do you have a topic or a question that you would like to be covered in an upcoming newsletter? Would you like to contribute on a topic? Please send any topics or questions to fpki-help@gsa.gov.