Protecting Federal High Value Assets

Business Brief

Benefits

Protect federal high value assets (HVAs) with endpoint artificial intelligence (AI) that evolves daily, preventing cyberattacks from ever being successful.

Examples of HVAs include:

- Servers with confidential personal information
- Web servers that host critical personally identifiable information
- Government employee PCs with public records
- PCs or servers with national security information

What It Is

Federal agencies across the United States are focused on identifying their HVAs to ensure they are kept safe from cybercriminals while also complying with the U.S. Office of Management and Budget (OMB) HVA guidelines. In an effort to protect all federal IT assets, encourage cross-agency cooperation in protecting HVAs, and update legacy infrastructure that is difficult to protect, the Obama administration developed the Cybersecurity National Action Plan (CNAP)[1]. This long-term plan aims to enhance cybersecurity protection and secure government computing assets. To enable near-term progress on the CNAP, the OMB issued guidance[2] for agencies to plan, identify, categorize, prioritize, report, assess, and remediate HVAs, and requires them to do this assessment, at a minimum, annually.

HVAs Defined

HVAs can be any of a wide array of hardware, software, data, and even processes; it's up to each agency to make their determination. Taken directly from the OMB memo, HVAs are defined as:

> *"assets, Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. HVAs may contain sensitive controls, instructions, data used in critical Federal operations, or unique collections of data (by size or content), or support an agency's mission essential functions, making them of specific value to criminal, politically motivated, or statesponsored actors for either direct exploitation or to cause a loss of confidence in the U.S. Government."*

Who Is Affected

Per the OMB, all federal agencies are affected by the requirements outlined in CNAP and must develop, maintain, and regularly update their HVA inventory lists on an annual basis at a minimum. Further, all federal agencies that fall under the CFO Act[3] are required to report all HVAs, including a prioritized top ten list, to DHS on an annual basis.

Federal agencies are targeted by cybercriminals and the amount of attacks is staggering. The Government Accountability Office testified that "security incidents reported by federal agencies …have risen from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014" and provided an exhaustive list of where cyberattacks originate, including other nations[4]. The report states that "several nations are aggressively working to develop information warfare doctrine, programs, and capabilities," and goes on to name China, Russia, Iran, and North Korea. In 2013, the Chinese military, specifically the People's Liberation Army General Staff Department, was implicated in a widespread cyberattack[5] program and the Department of Justice recently indicted two Russian Federal Security Service officers for their role in the enormous Yahoo attack[6]. The trend indicates that federal cyberthreats will not decrease in scale or in scope.

The successful incident response by the Office of Personnel Management (OPM) to the 2015 data breach attack, which included engaging Cylance®, demonstrates how organizations can react to, mitigate, and future-proof against similar HVA security breaches.

Certified for federal engagement, Cylance is a valued partner for protecting federal HVAs and ensuring compliance with the OMB guidelines.

Among the many federal cyberattacks that are publicly known, a few high profile security failures underscore the need for the U.S. to adopt near-term strategies and a long-term plan:

- **2015 Office of Personnel Management Data Breach:** A massive breach exposed the personal information of as many as four million federal employees
- **2015 Internal Revenue Service Data Breach:** More than 700,000 social security numbers and other sensitive information may have been stolen
- **2016 Federal Bureau of Investigation (FBI) Data Breach:** Attackers published contact information for 20,000 FBI employees just one day after posting similar data on almost 10,000 Department of Homeland Security employees

While HVA assessment can be time consuming, agency CIOs can quickly prevent many cybersecurity threats by securing their endpoints.

How Cylance Can Help

The human interaction element at most endpoints renders them the weakest link in any security chain. The endpoint, a foundational element in many HVAs, can be secured with AI based advanced endpoint protection that predicts and prevents attacks before they can execute.

Numerous federal agencies have already protected thousands of endpoints throughout their data centers with CylancePROTECT®. Using machine learning to predict, prevent, and stop malware and cyberattacks, Cylance AI recognizes how attackers attempt to exploit computers and thus can stop attacks before they can execute.

- Read more about Cylance's work with the OPM.
- Discover how Cylance protects federal HVAs.
- Want to know if you've been breached? Engage Cylance Consulting for a Compromise Prevention Assessment to determine if a security breach has happened or is actively occurring in your environment.

[1] White House press release, "FACT SHEET: Cybersecurity National Action Plan," February 9, 2016

[2] Memorandum M-17-09, "Management of Federal High Value Assets," December 9, 2016

[3] Per 31 U.S.C § 901(b), as amended, the current CFO Act agencies include the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, DHS, Housing and Urban Development, Interior, Justice, Labor, State, Transportation, the Treasury, Veterans Affairs, Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, OPM, Small Business Administration, Social Security Administration, U.S. Agency for International Development, and U.S. Nuclear Regulatory Commission.

[4] "INFORMATION SECURITY Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies," July 8, 2015, GAO Testimony Before the Subcommittees on Research and Technology and Oversight, Committee on Science, Space, and Technology, House of Representatives

[5] "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," February 18, 2013, New York Times

[6] "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," March 15, 2017, Department of Justice

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

©2017 Cylance Inc. Cylance® and CylancePROTECT® and all associated logos and designs are trademarks or registered trademarks of Cylance Inc. All other registered trademarks or trademarks are property of their respective owners.

20170516-1130