Continuous Monitoring and Enforcement under FISMA

Presidential Executive Order 13800 (EO), “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure” mandates each agency head use the NIST CSF to manage agency cybersecurity risk. The Cybersecurity Framework was created to provide high-level guidance for improving cybersecurity defenses with the understanding that many specific controls and processes are contained within existing adopted frameworks such as FISMA.

Three Security Control Strategies to help Address Risk, Meet FISMA, and Achieve Quick Wins

To achieve FISMA compliance, many organizations use the Risk Management Framework (RMF), described in NIST SP 800-37, continuous monitoring recommendations listed in NIST SP 800-137, and rely on NIST SP 800-53 for the full breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate. This “Build It Right” strategy is coupled with a variety of security controls for “Continuous Monitoring” giving organizations near real-time information for senior leaders making ongoing risk-based decisions affecting their critical missions and business functions. By integrating the NIST CSF, organizations create an overlay to their security strategy that will help prioritize higher-value assets and identify the greatest risk of intrusion.

Through proactive detection methods, advanced threat protections, and security automation, Carbon Black defends Federal information systems by continually monitoring and enforcing the integrity of critical assets by protecting configuration settings, software applications, and operating systems from unintended or malicious modification, ensuring that your endpoints and servers always operate as intended, are protected from advanced threats, and meet FISMA and EO guidelines for operational integrity and auditability.

Below are three control strategies listed in the Center for Internet Security's (CIS) Critical Security Controls (CSC, formerly the Consensus Audit Guidelines, CAG), mapped to NIST SP 800-53 and the NIST CSF that you can use to gain quick wins in your risk and security strategy to meet FISMA and EO mandates using Carbon Black.
Quick Wins

- Establish and ensure the use of standard secure configurations of your operating systems.
- Building a secure, “golden” image that is used to build all new systems.
- Validate with integrity checking tools capable of continuous inspection and change management to ensure that only authorized changes to the images are possible.

Carbon Black ensures that your device and software configurations do not drift from acceptable values through a combination of several different techniques:
- File Integrity Monitoring and Control
- Registry Protection
- Software & Configuration Drift Reports

Secure Configurations

- **CSC Control 3:** Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- **NIST SP 800-53 Controls:** CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, CM-10, CM-11, RA-5, CA-2, CA-7, SI-2, SI-3, SI-4, SI-5
- **NIST CSF Subcategory:** DE.AE-1, DE.AE-3, DE.CM-1, DE.CM4, DE.CM-7, DE.CM-8, DE.DP-2, DE.DP-5, ID.RA-1, PR.DS-7, PR.IP-1, PR.IP-3, PR.IP-12, PR.PT-3, RS.MI-3

Computers are inherently open systems, and all it could take is the modification of one setting to make a system vulnerable. Fortunately, though, there are well-known best practices for hardening systems that have been put into practice. One such practice is [The United States Government Configuration Baseline (USGCB)](https://doi.org/10.17255/IAccession=142967).
Quick Wins

- Devise a list of authorized software and version that is required in the enterprise and monitor with file integrity checking tools to validate that the authorized software has not been modified.
- Deploy application whitelisting technology that allows systems to run trusted software only.
- Perform regular scanning for unauthorized software and generate alerts when it is discovered on.

Carbon Black provides visibility, knowledge, and control over all the software running on every endpoint and server in the environment.

- Software Inventory System with Automated Reports
- Application Whitelisting
- Reports on Authorized and Unauthorized Software and Execution Attempts
- Consolidated Threat Intelligence, Software Reputation Services with Threat Assessment Reports.

Authorized Software

- **CSC Control 2**: Inventory of Authorized and Unauthorized Software
- **NIST SP 800-53 Controls**: CA-2, CA-7, CM-2, CM-6, CM-8, SI-4
- **NIST CSF Subcategory**: DE.AE-1, DE.AE3, DE.CM-1, DE.CM-7, DE.CM-8, DE.DP-2, DE.DP-5, ID.AM-2, ID.RA-1, PR.IP-1

It’s critical that Federal IT security staff know every piece of software running on every machine, be able to quickly assess its risk, and finally exercise pre-emptive control over whether the software can run or not. A smart whitelisting strategy does more than simply prevent the execution of unauthorized software; it acts as a last line of defense so that even if something does penetrate outer defenses, it will do no harm because it is not allowed to run in the first place.
Quick Wins

- Deploy an automated asset inventory discovery tool.
- Using a Dynamic Host Configuration Protocol with an asset inventory tool.
- Monitor and automate new asset inventory.

Carbon Black's Device Control capabilities enable tough yet flexible controls for managing storage devices and data transfer.

- Device Inventories and Audits
- Read/Write/Execute Control
- Storage Device Reports

Carbon Black gives you these essential controls to maintain operational effectiveness and compliance.

Cb Protection ensures policy enforcement by only allowing approved and compliant processes to run in your environment.

Cb Response allows you to trace the entire time line of an event and make key remediation steps within a fraction of the time typical forensics and imaging software can.

Controller Devices

- **CIS Control 1:** Inventory of Authorized and Unauthorized Devices
- **NIST SP 800-53 Controls:** CA-2, CA-7, CM-2, CM-6, CM-8, SI-4
- **NIST CSF Subcategory:** DE.AE-1, DE-AE3, DE.CM-1, DE.CM-7, DE.CM-8, DE.DP-2, DE.DP-5, ID.AM-2, ID.RA-1, PR.IP-1

Portable storage devices represent an enormous threat vector for the Federal Government for two reasons. First, they can act as a vehicle to bring unauthorized software into the network, bypassing many of the gateway-based security systems. Second, they represent a convenient and difficult-to-track way of extracting data from the information network and leaking it out of the organization.

Carbon Black provides the most advanced control over your information systems to protect your critical assets from today’s most advanced threats, in line with CSC practices, FISMA and EO guidelines to;

- Continuously monitor and measure the effectiveness of existing security controls,
- Prioritize high-risk areas that need to be addressed to meet policy,
- Get a true measurement of your security posture for the DHS and OMB.

To learn more about endpoint security solutions for the federal government, please visit [www.carbonblack/federal](http://www.carbonblack/federal)