FISMA Blog Post

Federal Cybersecurity: Administration Releases Annual Report on Agency Cyber Performance

By: Grant Schneider

Today the Administration is releasing the Fiscal Year (FY) 2016 Federal Information Security Modernization Act of 2014 (FISMA) Annual Report to Congress in accordance with 44 U.S.C. § 3553. The FISMA Report to Congress is the seminal Federal report on cybersecurity. This Report describes the state of Federal cybersecurity, including agency performance against key cybersecurity metrics, the independent reviews of the agency Inspectors General, cybersecurity policy and program updates, and a summary of cybersecurity incidents at agencies in accordance with the FISMA statute.

This year's Annual Report structure promotes transparency and enhances accessibility to information on the unique missions, resources, and challenges of each agency. The Report highlights agencies' performance improvements across several key cybersecurity areas, including agency implementation of:

- Information Security Continuous Monitoring capabilities that provide situational awareness of the computers, servers, applications, and other hardware and software operating on agency networks.

- Multi-factor authentication credentials that reduce the risk of unauthorized access to data by limiting users' access to the resources and information required for their job functions.

- Anti-Phishing and Malware Defense capabilities that reduce the risk of compromise through email and malicious or compromised web sites.

While Federal agencies continued to make progress in strengthening their cyber defenses in FY 2016, a significant amount of work remains to implement these controls and protect Federal networks and data. In fact, agencies reported 30,899 cybersecurity incidents to the Department of Homeland Security's (DHS) U.S. Computer Emergency Readiness Team (US-CERT) in FY 2016. In FY 2016, US-CERT's revised Incident Notification Guidelines required agencies to use an incident reporting methodology that classifies incidents by the method of attack, known as attack vector, and to specify the impact to the agency. This is a shift from the previous reporting methodology, where agencies reported on types of incidents that had no potential impact on operations. While the shift to attack vector means that the FY 2016 incident data is not comparable to prior years' incident data, the new approach allows OMB, DHS, and agencies to focus on incidents that may impact operations.. Similarly, the Report also details sixteen of the 30,899 incidents that agency heads determined were major information security incidents, a designation that triggers mandatory steps for agencies including reporting certain information to Congress.

The FISMA Report also provides a summary of the Inspector General (IG) community's revised methodology for assessing agency performance. The new methodology leverages the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity, which provides a common structure for public and private sector entities to identify and manage cybersecurity risks. The revised methodology provides greater context than prior Inspectors General assessments and helps stakeholders understand agency-specific challenges through this common structure.

Grant Schneider is the Acting Federal Chief Information Security Officer