



## OFFICE OF THE INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY NEWS RELEASE

### **The Office of the Inspector General of the Intelligence Community Completes FY 2018 Independent Evaluation of the Office of the Director of National Intelligence's Information Security Program and Practices, as Required by the Federal Information Security Modernization Act of 2014**

**(February 2019)** The Office of the Inspector General of the Intelligence Community (ICIG) recently completed the *FY 2018 Independent Evaluation of the Office of the Director of National Intelligence's (ODNI) Information Security Program and Practices, as Required by the Federal Information Security Modernization Act of 2014 (FISMA)* (AUD-2018-004). FISMA, introduced for the purpose of reducing security risk to federal information and data, provides a framework for the effectiveness of information security controls for Federal information systems. The ICIG's assessment of the effectiveness of ODNI's information security program and policies for Fiscal Year (FY) 2018 is classified. The ICIG identified deficiencies and made 11 recommendations.

FISMA requires federal agencies to establish agency-wide, risk-based security programs for the information systems that support the agency, including those systems provided or managed by another agency or operated by contractors. FISMA prescribes an annual process of self-assessment and independent evaluation of an agency's information security program and practices. Independent evaluations of the security of national security systems are integral for IC elements to ensure the protection of classified data and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The ICIG performs this annual independent evaluation of ODNI.

The objective of the evaluation was to assess the effectiveness and maturity of ODNI's information security program and practices. ICIG performed this evaluation using the *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, version 1.0 (*FY 2018 IG FISMA Reporting Metrics*), developed by the Office of Management and Budget, Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE). The ICIG assessed ODNI information security policies, procedures, and practices against the five information security function areas outlined in the National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1 (Cybersecurity Framework, April 16, 2018), using the maturity model developed by CIGIE.

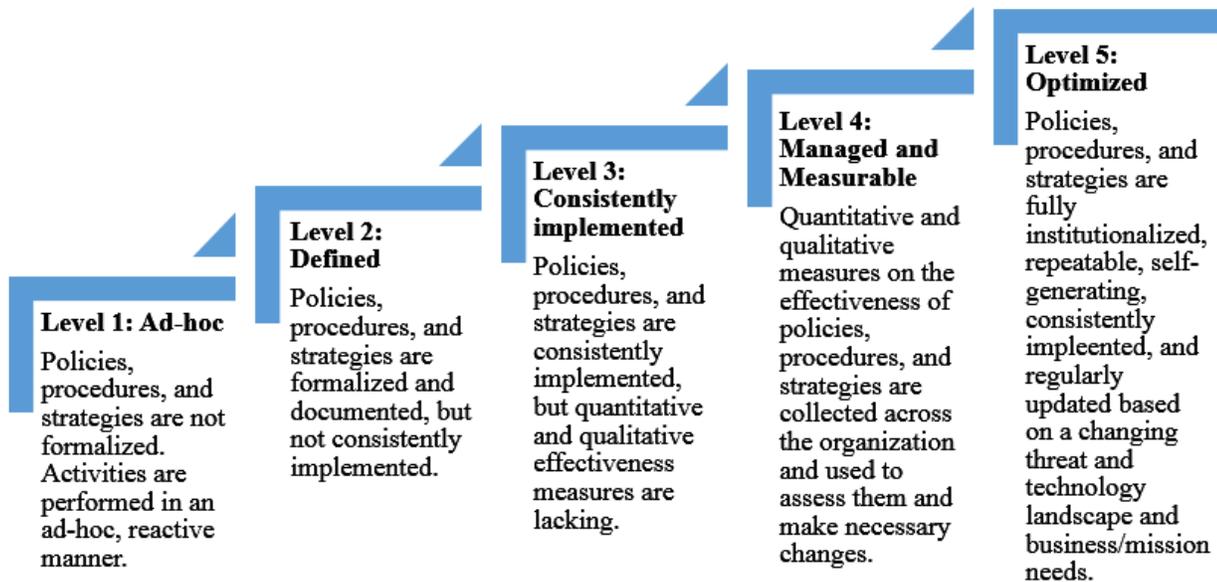
The *FY 2018 IG FISMA Reporting Metrics* requires 67 metric questions be addressed; the metrics align to eight information security domains that align with the five information security function areas in the NIST Cybersecurity Framework ([see Table 1](#)).

**Table 1: Cybersecurity Framework Function Areas and Related FISMA Domains**

Cybersecurity Framework Function Areas	FISMA Domains
<b>Identify:</b> Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	Risk Management
<b>Protect:</b> Develop and implement appropriate safeguards to ensure delivery of critical services.	Configuration Management
	Identity and Access Management
	Data Protection and Privacy
	Security Training
<b>Detect:</b> Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.	Information Security Continuous Monitoring
<b>Respond:</b> Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.	Incident Response
<b>Recover:</b> Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.	Contingency Planning

The *FY 2018 IG FISMA Reporting Metrics* requires Inspectors General to assess the effectiveness of information security programs on a maturity model spectrum, in which the foundational levels ensure that agencies develop sound policies and procedures and the advanced levels capture the extent that agencies institutionalize those policies and procedures. Figure 1 presents the five-level scale for assessing the development and implementation of controls for the five Cybersecurity Framework function areas. According to the *FY 2018 IG FISMA Reporting Metrics*, an information security program assessed at “Level 4—Managed and Measurable” is operating at an effective level of security at the domain, function, and overall program level.

**Figure 1: IG Evaluation Maturity Levels**



The Executive Summary and Appendix E (FY 2018 Intelligence Community FISMA Maturity Assessment Reporting Matrix) of the ICIG’s report will be provided to the Office of Management and Budget (OMB). In accordance with FISMA, the Director of OMB is responsible for summarizing FISMA reports from Intelligence Community agencies and submitting to Congress an annual report on the effectiveness of information security policies and practices relating to national security systems.

---

The Intelligence Authorization Act for Fiscal Year 2010 established the Office of the Inspector General of the Intelligence Community within the Office of the Director of National Intelligence. The ICIG’s mission is to provide independent and objective oversight of the programs and activities within the responsibility and authority of the Director of National Intelligence, to initiate and conduct independent audits, inspections, investigations, and reviews, and to lead and coordinate the efforts of the Intelligence Community Inspectors General Forum. The ICIG’s goal is to have a positive and enduring impact throughout the Intelligence Community, to lead and coordinate the efforts of an integrated Intelligence Community Inspectors General Forum, and to enhance the ability of the United States Intelligence Community to meet national security needs while respecting our nation’s laws and reflecting its values. The Forum consists of the twelve statutory and administrative Inspectors General having oversight responsibility for an element of the Intelligence Community. The Chair of the Forum is the Inspector General of the Intelligence Community.

For more information about the ICIG, please contact [IC IG PAO@dni.gov](mailto:IC_IG_PAO@dni.gov) or visit the ICIG’s websites:

Secure: <https://go.ic.gov/ICIG> | Unclassified: <https://www.dni.gov/icig>

For career opportunities with the ICIG, please visit:

Secure: <https://go.ic.gov/ICIGjob> | Unclassified: <https://www.dni.gov/careers>

To report allegations of waste, fraud, or abuse, please contact the ICIG:

Secure: ICIG Hotline 933-2800 | Unclassified: ICIG Hotline 855-731-3260

Secure Email: [ICIGHOTLINE@dni.ic.gov](mailto:ICIGHOTLINE@dni.ic.gov) | Unclassified Email: [ICIGHOTLINE@dni.gov](mailto:ICIGHOTLINE@dni.gov)