

Spotlight

Department of Homeland Security



Office of Inspector General

February 2014 OIG-14-43

Why This Matters

The Council of the Inspectors General on Integrity and Efficiency (CIGIE) Cybersecurity Working Group was charged with undertaking a review in which it would examine the role of the Inspector General community in current Federal cybersecurity initiatives. The high-level guide developed is based on the subject matter expertise of DHS OIG information technology audit managers and specialists, legal research, and a review of applicable websites and audit programs developed within the OIG community. The intent of this guide is to provide underlying policies and guidance and a foundation for conducting cybersecurity and information systems security-related audits.

Management Advisory Report: *A Guide for Assessing Cybersecurity Within the Office of Inspector General Community*

What We Determined

We collected cybersecurity and information technology system audit plans and programs from several agency OIGs. These plans and programs, in part, are consolidated in this guide. The guide will assist information technology auditors in evaluating the cybersecurity policies, practices, and system security controls implemented to protect Federal computer systems and networks from cyber threats and vulnerabilities. It also cites established policies and guidance that can be used to evaluate critical information technology security controls.

The guide is divided into seven sections. The first section outlines Federal agency cybersecurity roles and responsibilities. The second section covers cybersecurity policies and guidance for evaluating critical information technology security controls. The next section focuses on guidance regarding the use of vulnerability assessments and penetration testing Inspector General audit organizations can perform to evaluate the effectiveness of the system security and access controls implemented, and determine how well systems are protected when subject to attacks. The fourth and fifth sections cover information security continuous monitoring and cloud computing respectively. The sixth section consists of program steps for evaluating an agency's cybersecurity program and initiatives. The last section outlines program steps for conducting information system security-related audits and evaluations.

For Further Information:

Contact our Office of Public Affairs at (202)254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov