CIGIE Issues First-Ever Capstone Report on Trends in Federal Agencies’ Cybersecurity Performance


Cybersecurity risk management, or ensuring an effective information security program, continues to rank among the top management and performance challenges facing Federal agencies. For nearly 25 years, individual inspectors general (IGs) have performed independent evaluations of their respective agencies’ information security programs, as required by FISMA and predecessor legislation, such as the Government Information Security Reform Act of 2000 and the Federal Information Security Management Act of 2012. This cross-cutting report, published by CIGIE’s Technology Committee, marks the first time CIGIE has examined FISMA reports from OIGs across the Federal government to identify and analyze common Federal agency challenges.

While Federal agencies have improved their information security programs, the report notes that additional enhancements are needed in the areas of supply chain risk management, cybersecurity risk management, and configuration management. Continued improvements in these areas will better position Federal information security programs to identify, protect, detect, respond, and recover from advanced cybersecurity threats.

“This comprehensive cybersecurity report from CIGIE’s Technology Committee supports our efforts to highlight issues that cut across the Federal government,” said the Honorable Mark Lee Greenblatt, CIGIE Chairperson and Inspector General of the U.S. Department of the Interior. “CIGIE is committed to providing similar cross-cutting studies to Federal managers and policymakers, which can improve government operations and benefit the American public.”

The report is available at Oversight.gov, a publicly accessible, searchable website containing the latest public reports from Federal OIGs, who are members of CIGIE.

For additional information, please contact Andrew Cannarsa, Executive Director, CIGIE, at (202) 292-2603, or andrew.cannarsa@cigie.gov.