Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY

October 17, 2013

The Honorable Michael McCaul
Chairman, Committee on
Homeland Security
U.S. House of Representatives
Washington, DC 20515

The Honorable Bennie Thompson
Ranking Member, Committee on
Homeland Security
U.S. House of Representatives
Washington, DC 20515

Dear Chairman McCaul and Ranking Member Thompson:

The Legislation Committee of the Council of the Inspectors General on Integrity and Efficiency (CIGIE) writes to express our views on behalf of the Inspector General (IG) community concerning pending information security legislation. On behalf of the Legislation Committee, I would like to describe the significant value Offices of Inspector General (OIGs) provide in conducting annual independent evaluations of federal agencies' information security programs and controls in individual information systems, pursuant to the Federal Information Security Management Act of 2002 (FISMA). In addition, I would like to offer specific comments on H.R. 1163, the *Federal Information Security Amendments Act of 2013*, which passed the House on April 16, 2013, and H.R. 1468, the *Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2013* (SECURE IT), which was introduced on April 10, 2013.

FISMA's Annual Independent OIG Evaluation Requirement Adds Significant Value Through OIG Identification of Agency Deficiencies and Necessary Corrective Actions

Since FISMA was enacted in 2002, OIGs have provided over a decade of oversight to help ensure federal agencies take action and have appropriate procedures in place to address information security vulnerabilities. Under FISMA's mandatory OIG evaluation requirement, OIGs government-wide have served as a fresh set of eyes and independent voice keeping agency heads and others focused on the adequacy of agency information security programs, including related controls in individual systems and the corrective actions needed. CIGIE believes maintaining FISMA's mandatory independent OIG evaluation requirement is critical to ensuring that agencies across the federal government are held accountable for their information security efforts. Additionally, this government-wide approach sends a strong message to agency security officials regarding the importance of having strong security controls that are properly designed and implemented, including structured processes and documented policies and procedures.

Over the past 10 years, OIG FISMA evaluations have identified a variety of information security deficiencies and vulnerabilities requiring necessary corrective actions by agencies. Under FISMA, the OIG community regularly evaluates the information security controls of individual agency systems throughout each year, making numerous recommendations to improve

agencies' system controls and information security programs and processes. Additionally, OIGs regularly examine key agency policies, procedures, and processes to determine whether such practices provide sufficient assurance that the agency's information and information systems are adequately secured.

The importance of the OIGs' FISMA work was recently presented in the Office of Management and Budget's (OMB's) *Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002* (2012 FISMA Implementation Report). OMB reported that while the majority of the 24 agencies covered by the Chief Financial Officers Act of 1990 (CFO Act) had programs in place for each information security area, independent OIG reports found many agencies lacked specific program components. For example:

- Nearly thirty percent of the agencies did not have documented strategies and plans for continuous monitoring.
- Two-thirds of the agencies did not have a fully developed patch management process and were not remediating findings from vulnerability scans in a timely manner.
- Fifty percent of the agencies did not ensure users were granted access based on needs and separation of duties.
- Fifty percent of the agencies had not established and adhered to milestone dates for remediating vulnerabilities or ensured remediation plans were effective for correcting weaknesses.
- One-third of the agencies did not obtain sufficient assurance that contractor-operated systems complied with FISMA requirements.

Although these statistics speak for themselves, CIGIE believes that OMB's 2012 FISMA Implementation Report highlights the critical nature of the OIGs' FISMA findings and reinforces the importance of continuing to require that each OIG perform an annual independent evaluation of its agency's information security program and practices.

H.R. 1163 and H.R. 1468 Should Be Amended to Maintain the Current FISMA Independent Evaluation Provisions

CIGIE strongly supports legislation to enhance the security and resiliency of the U.S. cybersecurity infrastructure, including the use of automated and continuous monitoring, which is particularly discussed throughout H.R. 1163. CIGIE strongly believes, however, it is equally important to ensure OIGs independently evaluate the adequacy of agencies' information security programs, practices, and controls, including continuous monitoring activities, through the current FISMA framework. OMB's 2012 FISMA Implementation Report highlights that automated and continuous monitoring is not enough to protect federal agencies' information security infrastructure. More needs to be done; for example, when approximately two-thirds of the agencies covered by the CFO Act lack a fully developed patch management process and do not remediate findings from vulnerability scans in a timely manner, it is critically important for OIGs to continue performing FISMA evaluations. CIGIE believes that such evaluations are the best way to ensure adequate information security practices and controls are in place, including

continuous monitoring processes, and that federal agencies take timely action to remediate identified vulnerabilities.

Therefore, for the reasons stated above, CIGIE recommends that both H.R. 1163, the *Federal Information Security Amendments Act of 2013*, and H.R. 1468, SECURE IT be amended to maintain the current OIG FISMA annual evaluation provisions. This amendment should include the statutory language found in 44 U.S.C. § 3545(a)(2) requiring each independent OIG evaluation to (1) test the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems and (2) assess agency compliance with the requirements of FISMA and other related information security policies, procedures, standards, and guidelines.

Additionally, while both H.R. 1163 and H.R. 1468 appropriately focus on requiring agencies to perform automated and continuous monitoring, CIGIE believes OIG FISMA evaluations are an important independent check on the process that helps to ensure appropriate policies, procedures, and practices are in place for conducting continuous monitoring and to address any identified vulnerabilities. H.R. 1163 requires agencies to self-report their security vulnerabilities, which is a critical component of information security. CIGIE does not believe, however, that agency self-reporting is enough. Independent OIG FISMA reviews are a necessary addition to self-reporting to provide an independent check and ensure all information security issues are identified.

H.R. 1468 Should Be Amended Consistent with CIGIE's Statutory Mission and to Ensure OIGs May Perform FISMA Work as an Audit, Evaluation, or Other Review

In addition to its support for the current FISMA structure, CIGIE would also like to offer three comments specific to the provisions of H.R. 1468, which was introduced on April 10, 2013. First, section 106 states CIGIE is "authorized to review compliance by the cybersecurity centers, and by any Federal department or agency receiving cyber threat information from such cybersecurity centers, with the procedures requirement under section 102 of this Act." Under the Inspector General Reform Act of 2008 (IG Reform Act), CIGIE's role is to address integrity, economy, and effectiveness issues transcending individual government agencies, and to increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the OIGs. Functionally, key facets of CIGIE's role are to continually identify, review, and discuss areas of weakness and vulnerability in federal programs and operations with respect to fraud, waste, and abuse and to develop plans for coordinated, government-wide activities addressing these problems and promoting economy and efficiency. To that end, CIGIE is not charged with, or allocated independent resources to, conduct compliance or performance reviews. These types of reviews should be conducted by the OIG with jurisdiction for a specific department or agency. For similar reasons, CIGIE has concerns about H.R. 1468's amendment to section 3554(a)(4), which would require CIGIE and the Director of OMB to consult and designate an independent entity to perform FISMA reviews for those agencies with no Inspector General; CIGIE believes such activities would be inconsistent with the statutory duties and responsibilities that Congress envisioned for CIGIE in enacting the IG Reform Act.

Second, H.R. 1468 would amend 44 U.S.C. § 3556(a) to read: "The [CIGIE], in consultation with the Director and the Secretary of Homeland Security, the Secretary of Commerce, and the Secretary of Defense, shall issue and maintain criteria for the timely, cost-effective, risk-based, and independent evaluation of each agency-wide information security program (and practices) to determine the effectiveness of the agency-wide information program (and practices)." H.R. 1468 would also require that any such criteria include "measures to assess any conflicts of interest in the performance of an evaluation . . . ." As stated above, CIGIE prefers the criteria established by the existing version of FISMA. To the extent these criteria are amended, CIGIE believes the responsibility for establishing specific technical guidance for government-wide information security program evaluations would be better placed with an entity outside of CIGIE. Therefore, we suggest that a better approach would be to require the Department of Homeland Security to establish guidance "in collaboration with and with the approval of" CIGIE.

Third, H.R. 1468's FISMA amendments remove a critical piece of statutory language currently codified at 44 U.S.C. § 3545(d), which provides that any OIG evaluation conducted under FISMA "may be based in whole or in part on an audit, evaluation, or report related to programs or practices of the applicable agency." CIGIE members have stated this provision has been highly important because it makes it abundantly clear OIGs have the flexibility to perform FISMA-related work as an audit, evaluation, or other report. Section 3556(b) of H.R. 1468 could be narrowly interpreted to take away this flexibility and require OIGs to perform FISMA work as an "evaluation" without clearly defining the term, which could lead to needless claims by agency management attempting to limit the type of work OIGs do in this area. If the above-cited provision were to be inserted into H.R. 1468, it would clarify that OIGs continue to have the ability to perform this same work as an audit, evaluation, or other type of work, as appropriate. Additionally, current law makes it clear OIGs do not have to conduct one single FISMA audit or evaluation to comply with section 3545. Rather, the annual IG reporting requirement could be based on smaller audits or evaluations done throughout the year. For these reasons, CIGIE recommends that the language of 44 U.S.C. § 3545(d) be included in H.R. 1468.

H.R. 1163 and H.R. 1468 Should Be Amended to Hold Agencies Publicly Accountable While Properly Protecting Agency Information Security Vulnerabilities

Finally, CIGIE has expressed its view in the past concerning the importance of properly protecting specific and detailed information about an agency's information security vulnerabilities, while still ensuring agencies are held publicly accountable. H.R. 1468 recognizes the importance of protecting such information by providing, at section 3556(a), that agency-wide information security programs include "appropriate safeguards against disclosure of information where such disclosure may adversely affect information security." To ensure agency information and OIG reports concerning vulnerabilities in the agency's information security infrastructure are properly protected, CIGIE recommends both H.R. 1163 and H.R. 1468 be amended to include the following statutory Freedom of Information Act (FOIA) exemption:

> Information related to a federal agency's information security program or practices shall be exempt from disclosure under section 552(b)(3) of title 5,

> United States Code, if disclosure could reasonably be expected to lead to or result in unauthorized (1) access, (2) use, (3) disclosure, (4) disruption, (5) modification, or (6) destruction of an agency's information system or the information that system controls, processes, stores, or transmits. Federal agencies' use of this section shall be conducted in accordance with an agency's obligation to reasonably segregate non-exempt information under 552(b) of title 5, United States Code.

We believe this provision would allow agencies to protect from public release information sensitive to their operations while at the same time preventing agencies from withholding non-sensitive information. This maintains the balance the FOIA seeks to achieve between the legitimate protection of agency information, and the need for public disclosure.

Thank you for considering the perspectives of CIGIE with regard to OIG FISMA evaluations, and the sections of H.R. 1163 and H.R. 1468 directly affecting the OIG community. If you have any questions or need additional information, please feel to contact me at (202) 205-6586.

Sincerely,

Peggy E. Gustafson
Inspector General, Small Business Administration
Chair, Legislation Committee
Council of the Inspectors General on
Integrity and Efficiency

Cc: Committee on Armed Services
Committee on Energy and Commerce
Committee on Judiciary
Committee on Oversight and Government Reform
Committee on Science, Space and Technology
Permanent Select Committee on Intelligence