Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY

April 24, 2012

The Honorable Ralph M. Hall
Chairman
Committee on Science, Space and Technology
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Eddie Bernice Johnson
Ranking Member
Committee on Science, Space and Technology
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Hall and Ranking Member Johnson:

The Legislation Committee of the Council of the Inspectors General on Integrity and Efficiency (CIGIE or the Council) is writing to express the Council's views on H.R. 4263, the *Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012* (SECURE IT), which was introduced on March 27, 2012.

In this time of rapid technological change, CIGIE fully supports the purpose of this legislation, which is to enhance the security and resiliency of the cyber and communications infrastructure of the United States. Based on the expertise and experience of the Inspector General (IG) Community, CIGIE offers the following comments on section 105, which is a new provision found in title I of the legislation, and section 3556, found in title II, section 201 of the legislation, which amends the Federal Information Security Management Act of 2002 (FISMA).

First, section 105 states that CIGIE "may review compliance by the cybersecurity centers, and by any Federal department or agency receiving cyber threat information from such cybersecurity centers, with the procedures required under section 102." Under the Inspector General Act of 1978, as amended (IG Act), CIGIE's role is to address integrity, economy, and effectiveness issues that transcend individual Government agencies; and 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 offices of the Inspectors General. 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 develop plans for coordinated, Government-wide activities that address these problems and promote economy and efficiency. To that end, CIGIE is not charged with or allocated independent resources to conduct compliance or performance reviews; rather, these types of reviews would be conducted by the Inspector General with jurisdiction for a specific department or agency.

Second, CIGIE prefers the criteria established by the existing version of FISMA for conducting independent IG evaluations of their respective agency's information security program

as contained in 44 U.S.C. 3545(a)(2) to the criteria set forth in section 3556 in the legislation. Under this section, IG evaluations are currently required to include (1) testing of the effectiveness of the agency's information security policies, procedures and practices based on a representative subset of the agency's information systems, and (2) an assessment of agency compliance that is based on the results of this testing. These criteria have served as a solid baseline for enhancing information security throughout the federal government.

Third, CIGIE recommends that one current FISMA provision that does not appear in the current legislation be inserted into H.R. 4263. In the provisions related to IGs' independent evaluations of agency information security programs, the current version of FISMA contains the following provision: "The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report related to programs or practices of the applicable agency." This language is currently codified at 44 U.S.C. § 3545(d). CIGIE members have stated that this provision has been highly important in the past because it provides IGs with the flexibility to perform FISMA-related work as an audit or an evaluation. H.R. 4263 currently requires IGs to perform its FISMA work as an "evaluation." If the above-cited provision were to be inserted into H.R. 4263, IGs would have the ability to perform this same work as an "audit," as necessary. Also, current law makes it clear that IGs do not have to do 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 44 U.S.C. § 3545(d) be included in H.R. 4263 as a new subsection under "3556. Independent Evaluations."

Fourth, CIGIE recommends amending H.R. 4263 to include a statutory Freedom of Information Act (FOIA) exemption that protects certain information that, if disclosed, would jeopardize an agency's information security system. In order to ensure IG reports concerning vulnerabilities in an agency's information security infrastructure are properly protected, CIGIE recommends that the bill be amended to include the following statutory exemption:

> Information that, if disclosed, would directly or indirectly jeopardize the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits shall be exempt from disclosure under 552(b)(3) of title 5, United States Code.

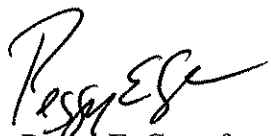
Finally, H.R. 4263 (page 50) requires CIGIE to "issue and maintain criteria for the timely, cost-effective, risk-based, and independent evaluation of each agencywide information security program" in consultation with the Director of the Office of Management and Budget, and the Secretaries of Homeland Security, Commerce, and Defense.

CIGIE believes that the responsibility to establish specific criteria for Government-wide information security program evaluations would be better placed with an entity outside of CIGIE. Therefore, we suggest that the provisions set forth in S. 413 (*The Cybersecurity and Internet Freedom Act of 2011*) requiring the Government Accountability Office (GAO) to establish guidance "in collaboration with" CIGIE is a better approach. We also recommend that

guidance be issued with the concurrence of CIGIE. While the OIGs have gained extensive knowledge of information security through more than a decade of FISMA audits and evaluations, GAO can incorporate important insights and analytical approaches for the OIG reviews based on its unique vantage point of monitoring information security across Government and reporting yearly on the status of information security.

Thank you for considering the perspectives of CIGIE with regard to the sections of H.R. 4263 that directly affect the IG Community. If you like to further discuss identifying an appropriate mechanism for compliance reviews of the cybersecurity centers or any other aspect of our comments and recommendations, please feel free 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