Council of the
INSPECTORS GENERAL
on INTEGRITY *and* EFFICIENCY

March 20, 2012

The Honorable John D. Rockefeller, IV
Chairman
Committee on Commerce, Science and Transportation
United States Senate
Washington, D.C. 20510

The Honorable Kay Bailey Hutchison
Ranking Member
Committee on Commerce, Science and Transportation
United States Senate
Washington, D.C. 20510

Dear Chairman Rockefeller and Ranking Member Hutchison:

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 certain provisions of S. 2105, the *Cybersecurity Act of 2012*, which was introduced on February 14, 2012, and S. 2151, the *Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012* (SECURE IT), which was introduced on March 1, 2012.

In this time of rapid technological change, the CIGIE fully supports the purpose of these pieces of 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 four comments on section 3556 of S. 2105 and S. 2151, which amend the Federal Information Security Management Act of 2002 (FISMA).

First, 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 and carried forward in section 3556 of S. 2105. These criteria have served as a solid baseline for enhancing information security throughout the federal government. We also recommend a technical amendment to the "Independent Evaluations" section of S. 2105 that would further enhance the IG's ability to conduct its work. Specifically, on page 79 (line 7), S. 2105 would amend FISMA to require that each IG's evaluation of an agency's information security program and practices include "a *conclusion* as to the effectiveness of the information security policies, procedures, and practices of the agency in addressing risk based on a determination of the aggregate effect of identified deficiencies."

CIGIE members have expressed concern about a requirement that Inspectors General reach a "conclusion" as to the effectiveness of an agency's information security program. S. 2105 does not establish particular criteria against which an IG can measure when reaching a conclusion as to the effectiveness of its agency's information security program. Moreover,

CIGIE members have expressed concern about whether a fluid discipline such as information security can have definitive criteria on which to base a finite conclusion. Even if criteria for such a conclusion were established, it should also be noted that a mandate to formulate such an "opinion" would significantly increase the cost of performing a FISMA review, requiring additional OIG staff in offices that perform FISMA work and additional funds for increased contractor costs in offices that hire independent public accountants. CIGIE recommends changing the italicized word "conclusion" to "assessment." This change is consistent with other provisions in the "Independent Evaluations" section of S. 2105. For example, the second requirement for each IG evaluation, which is also found on page 79, states that IGs shall perform "an *assessment* of compliance" with subchapter II of chapter 35.

Second, CIGIE recommends that one current FISMA provision that does not appear in the current legislation be inserted into S. 2105. 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. S. 2105 currently requires IGs to perform its FISMA work as an "evaluation." If the above-cited provision were to be inserted into S. 2105, 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 S. 2105 as a new subsection under "3356. Independent Evaluations."

Third, CIGIE recommends amending S. 2105 and S. 2151 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 both bills 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.

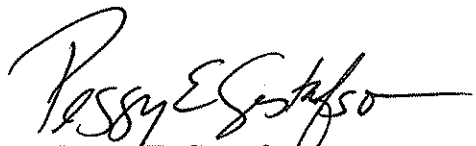
Fourth, S. 2105 (page 79) requires CIGIE to "issue and maintain guidance for performing timely, cost-effective, and risk–based evaluations under subsection (a)" in consultation with the Secretary of Homeland Security, the Comptroller General and the Director of the National Institute of Standards and Technology. S. 2151 (page 48) contains a similar requirement, though the requirement differs, in that CIGIE is directed to consult with the Director of the Office of

Management and Budget, and the Secretaries of Homeland Security, Commerce, and Defense in promulgating criteria for independent evaluations.

CIGIE believes that the responsibility to establish specific technical guidance for Government-wide information security program evaluations would be better placed with an entity outside of the CIGIE. Therefore, we suggest that the guidance provisions set forth in S. 413 (*The Cybersecurity and Internet Freedom Act of 2011*) requiring GAO to establish guidance "in collaboration with" CIGIE is a better approach. We also recommend that guidance be issued with the concurrence of the 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 S. 2105 and S. 2151 that directly affect the IG Community. If you have any questions or need additional information, please feel free to contact me at (202) 205-6586. We also have provided a copy of this letter to the Chairman and Ranking Member of the Committee on Homeland Security and Governmental Affairs.

Sincerely,



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