Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY

July 19, 2012

The Honorable Joseph I. Lieberman
Chairman
Committee on Homeland Security and
Government Affairs
United States Senate
Washington, D.C. 20510

The Honorable Susan Collins
Ranking Member
Committee on Homeland Security and
Government Affairs
United States Senate
Washington, D.C. 20510

Dear Chairman Lieberman and Ranking Member Collins:

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. 3342, the *Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012* (SECURE IT), which was introduced on June 27, 2012. This bill is similar to S. 2151, also called SECURE IT, to which CIGIE provided comments in letters to the Senate Committees on Homeland Security and Governmental Affairs and Commerce, Science, and Transportation on March 20, 2012. Some of the comments presented here reiterate comments made in those letters.

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 106 of Title I, which is a new provision that was not included in S. 2151; and on section 201 of Title II, which would amend the Federal Information Security Management Act of 2002 (FISMA) by adding section 3556 thereto.

First, section 106(a) states that 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 required under section 102 of this Act." Under the Inspector General Act of 1978, as amended, 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 neither charged with conducting, nor allocated independent

resources to conduct compliance or performance reviews; rather, these types of reviews would be conducted by the IG with jurisdiction over a specific department or agency. Therefore, we recommend that this section be deleted.

Second, section 3556(a) on pages 57 and 58 states that 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 agencywide information security program (and practices) to determine the effectiveness of the agencywide information security program (and practices).

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 CIGIE. Therefore, we suggest that the guidance 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 the guidance be issued with the concurrence of CIGIE. While the IG community has 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 IG reviews based on its unique vantage point of monitoring information security across Government and reporting yearly on the status of information security.

Third, section 3556(a) states that the criteria for conducting IG evaluations include "measures to assess any conflicts of interest in the performance of the evaluation." It is uncertain how assessing conflicts of interest would be incorporated into the scope of inquiry of such evaluations. Rather, CIGIE prefers the criteria established by the existing version of FISMA for conducting independent IG evaluations of each respective agency's information security program, including an assessment of agency compliance with FISMA, as contained and carried forward in section 3556 of S. 2105 (*Cybersecurity Act of 2012*), with the exception that the word "conclusion" be replaced with "assessment" in section 3556(b)(3). 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. The criteria carried forward in section 3556 of S. 2105 have served as a solid baseline for enhancing information security throughout the federal government.

Also, the criteria in section 3556(a) include "whether the agencywide information security program includes appropriate safeguards against disclosure of information where such disclosure may adversely affect information security." CIGIE believes that in order to achieve this objective, the bill should include a specific statutory exemption that, in accordance with the Freedom of Information Act, protects certain information that, if disclosed, would jeopardize an agency's information security system. Therefore, in order to ensure agency information and 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 section 552(b)(3) of title 5, United States Code.

Finally, CIGIE recommends that one current FISMA provision that does not appear in the current legislation be inserted into S. 3342. 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. 3342 currently requires IGs to perform its FISMA work as an "evaluation." If the above-cited provision were to be inserted into S. 3342, IGs would have the ability to perform this same work as an "audit," as appropriate. 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. 3342 as a new subsection under "§ 3556. Independent Evaluations."

Thank you for considering the perspectives of CIGIE with regard to the sections of S. 3342 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 Chairman and Ranking Member of the Committee on Commerce, Science, and Transportation.

Sincerely,

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