

INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

*Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]*

July 31, 2012

The Honorable Jeffrey Zients
Acting Director
US Office of Management and Budget
Washington, DC 20502

Dear Mr. Zients,

I am writing to you as the Chair of the Information Security and Privacy Advisory Board (ISPAB). The ISPAB was originally created by the Computer Security Act of 1987 (P.L. 100-35) as the Computer System Security and Privacy Advisory Board, and amended by Public Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act (FISMA) of 2002. One of the statutory objectives of the Board is to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy.

At the Board's meeting of May 31, 2012, industry and government panelists spoke about various methods and institutions for sharing information about cyber threats and indicators, affecting the integrity and operability of federal and private sector information and communications systems. The discussion showed that many organizations dedicated to information sharing, such as the NCCIC (National Cyber and Communications Integration Center) and the DSICE (Defense Industrial Base (DIB) Collaborative Information Sharing Environment), continue to have high potential, but must address numerous policy and operational issues before they reach full potential.

The Board also heard about the model of the National Cyber Forensics and Training Alliance (NCFTA), which is taking action to determine applicability to expedite both human and automated sharing overall, and could serve as a model for similar efforts in cyber information sharing.

The Board also heard about assessments of the DIB Pilot, which enabled the use of classified threat intelligence to filter Internet traffic to and from pilot participants in industry and government. The pilot showed some positive results in the view of both government and industry participants, and sufficient promise that it should be considered and improved for

application to critical infrastructure sectors outside of defense. To reach other sectors would require greater reliance on classified information --which, it was noted, can often be reduced to an unclassified indicator (such as an integer on a spectrum from "no threat" to "big threat") for use in a non-classified automated sharing environment. Future automated sharing initiatives in any environment can leverage lessons learned under the DIB pilot model by:

1. ensuring clarity and mutual agreement on specific information needs;
2. focusing on improving timeliness and accuracy of data;
3. establishing consistent cyber information sharing processes across agencies, so that indicators can be received and treated consistently; and
4. promoting a sharing network based on a trust framework.

Accordingly, the Board concluded that the Administration should engage more actively with the private sector to consider enhanced means for automated information sharing. A greater knowledge of the condition at each node where commercial and government networks come together will enhance abilities to filter out malicious traffic and prevent threats from reaching targets. This knowledge can come from combining currently disparate threat pictures for companies and agencies, to integrate situational awareness and provide threat indicators without sacrificing intellectual property or requiring classified information.

Working in milliseconds at real-time, rather than always relying on human intervention, can minimize time and mitigate many of the legal, policy, privacy and trust concerns that hamper full effectiveness of "human-to-human" information sharing. That said, human and machine collaboration are symbiotic; greater use of automated indicator exchange can also foster a byproduct of additional combined intelligence that can be used in human decisioning.

One example of an existing mechanism that can be tapped for private sector use is the Managed Trusted Internet Protocol Service (MTIPS) program, and the associated managed security services offered by some ISPs that have already invested in the DIB pilot infrastructure and process. There may also be other options to explore according to any unique attributes of specific participating sectors.

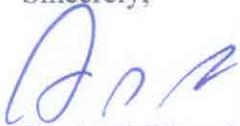
Based on our discussions, the ISPAB offers several recommendations:

- OMB and relevant federal agencies should consult with the private sector to assess the policy and operational issues, including longer term R&D needs, associated with developing robust automated cyber threat and indicator information sharing between government and the private sector, and to consider potential impacts of indemnification and liability protections for the private sector in sharing information for cyber security.

- Policies, processes and technologies for automated indicator sharing should be designed with privacy integral to functionality, with well-defined limitations of use around data to enable fast, needed, urgent and abundant use of cyber situational awareness data.
- Public awareness campaigns can educate stakeholders on the types of data used for cyber security situational awareness, to differentiate from other types of data collection used for activities such as marketing. Cybersecurity stakeholders would also benefit from education about the fact that no cyber sharing network is perfect – in a world where there will always be some level of loss, the key question is how much risk agencies should assume for such losses.

The Board appreciates the opportunity to provide our views.

Sincerely,



Daniel J. Chenok
Chairman
Information Security and Privacy Advisory Board

cc: Steve VanRoekel, Administrator of E-Government and Information Technology and CIO,
OMB
Michael Daniel, Cybersecurity Coordinator, National Security Council,
Mark Weatherford, Deputy Undersecretary for Cybersecurity, DHS
Patrick Gallagher, Director, NIST