Attorneys:

- **Timothy G. Ronan**
  tronan@pullcom.com
  203.674.7933

CYBER LAW TRACKER: January 2011

The Latest in Cybersecurity and Infrastructure Protection Legal Developments

IT'S REPORT CARD TIME FOR THE OBAMA ADMINISTRATION'S CYBERSECURITY POLICY

by T. Scott Cowperthwait, Posted on January 26, 2011

Last week, the National Security Cyberspace Institute, Inc. (NSCI) released a whitepaper entitled "Federal Government Cybersecurity Progress: Obama Administration Report Card 2009-Present." In the whitepaper, NSCI examined the Obama administration's cybersecurity record against the recommendations contained in the Cyberspace Policy Review released in May 2009. NSCI specifically targeted the Obama administration's response to the ten recommendations contained in the Near-Term Action Plan, as opposed to the fourteen recommendations contained in the Mid-Term Action Plan. Utilizing an A through F grading system, NSCI assigned the Obama administration with four Bs, four Cs and two Ds. Check out the link below to the whitepaper for NSCI's explanation for each grade and additional observations and recommendations.

Source: http://nsci-va.org/WhitePapers/2011-01-18-Federal%20Government%20Cybersecurity%20Progress-Crouch-McKee-Keys.pdf

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL RELEASES INFORMATION SHARING STUDY

by T. Scott Cowperthwait, Posted on January 20, 2011

On January 18, 2011, the National Infrastructure Advisory Council (NIAC), which provides the president, through the secretary of homeland security, with advice on the security of critical infrastructures, received an update to its working group's study on intelligence information sharing between the public and private sectors. The update, which was provided at an NIAC public meeting, comes in response to the President's request last spring that the NIAC form a working group to review and assess the current view of intelligence information sharing between the government and infrastructure owners and operators, and identify progress, gaps and recommendations for improvement. The working group has identified the following areas of review for its study:

1. A review of intelligence information sharing, addressing issues such as the timeliness and relevance of information and intelligence shared between the public and private sector and bi-directional processes and products shared between government and the private sector;

1. Enhancing owner and operator contributions to counterintelligence, addressing issues such as the private sector role in counterintelligence and challenges and potential solutions to improving contributions by owners and operators; and
1. The role of fusion centers, addressing private sector participation and interaction, as well as information sharing challenges, gaps and best practices.

According to the update, the study is examining the diverse operating cultures of different sectors, including the chemical, commercial facilities, health care and public health oil and natural gas and financial services sectors, using several case studies in order to help frame multiple models for public and private sector information sharing. The NIAC working group has recommended that it take the following next steps:

1. A review of current federal policy, programs and plans through briefings, interviews and open-source research to establish baseline conditions with respect to intelligence/counterintelligence assessments;

1. Sector-specific case studies focusing on the framework for information sharing and reviewing what information is being shared in order to identify potential gaps; and
1. Identifying the initial set of issues related to private sector participation and interaction in fusion centers and the initial set of information sharing challenges, gaps and best practices.

After the NIAC reviews and deliberates on the working group's update, it will provide further direction to the working group on how it should proceed. Stay tuned for more details.

Source: http://www.dhs.gov/xlibrary/assets/niac/niac-information-sharing-study-presentation-2011-01-18.pdf

Source: http://www.dhs.gov/xlibrary/assets/niac/niac-brochure-update-2010-11-24.pdf

ENERGY SECTOR FACES ALARMINGLY HIGH RISK OF CYBER ATTACK

by T. Scott Cowperthwait, Posted on January 18, 2011

At the end of 2010, Deloitte & Touche LLP examined the rising cybersecurity threat facing the energy sector. According to Deloitte's study, malware intrusions and cyber attacks against energy companies target critical assets, including intellectual property, personal identifiable information and critical infrastructure assets. The result of such intrusions and attacks is that the energy sector, specifically oil and gas companies, incur the "second-highest cyber-crime costs" associated with cybersecurity. Deloitte proposes that energy companies abandon the old, reactionary approach for information security and, instead, develop proactive cybersecurity programs.

The U.S. Department of Homeland Security Energy Sector-Specific Plan to the National Infrastructure Protection Plan (2010) advocates for the implementation of sector-specific goals focused on critical infrastructure protection, including: 1) information sharing and communication among trusted public and private sector partners; 2) physical and cyber security to enhance preparedness, security and resilience; 3) coordination and planning to enhance reliability and emergency planning; and 4) strengthening private and public confidence in the sector's ability to manage risk and implement effective security, reliability and recovery efforts. The 2010 Energy-Sector Specific Plan identifies several cyber asset protection issues and priorities in line with Deloitte's review. For example, the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) Reliability Standards address multiple aspects of cyber asset protection for the electricity sub-sector, including: 1) data and information classification according to confidentiality; 2) identification and protection of cyber assets related to reliable operation of the bulk electric systems; and 3) annual approval by senior management of the risk-based assessment methodology in addition to the list of critical cyber assets. The oil and gas subsector has identified the following priorities: 1) assess security vulnerabilities at single-point assets such as refineries, storage terminals and other buildings, as well as networked features such as pipelines and cyber systems; and 2) work toward resilient, secure cyber networks and SCADA systems in order to detect and respond to cyber attacks.

With the Deloitte study and 2010 Energy-Sector Specific Plan in mind, energy companies should be conducting threat vulnerability assessments to identify cybersecurity capability gaps in their cybersecurity programs.

Source: http://www.ogj.com/index/blogs/health-safety-environment/blogs/OGJ/health-safety-environment-blog/post987_4431226202297142623.html

Source: http://www.deloitte.com/view/en_US/us/Insights/Browse-by-Content-Type/dbriefs-webcasts/Industries/Oil-Gas/cf38079b3cdea210VgnVCM1000001a56f00aRCRD.htm

Source: http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf

OBAMA ADMINISTRATION CYBERSECURITY TEAM ANNOUNCES “IDENTITY ECOSYSTEM” TO BE DEVELOPED AND OVERSEEN BY THE U.S. DEPARTMENT OF COMMERCE

by T. Scott Cowperthwait, Posted on January 14, 2011

This week, Cybersecurity Coordinator and Special Assistant to the President Howard A. Schmidt and U.S. Commerce Secretary Gary Locke announced the formation of a National Program Office within the U.S. Department of Commerce to help coordinate federal activities to implement the National Strategy for Trusted Identities in Cyberspace (NSTIC). The NSTIC seeks to create an “Identity Ecosystem” designed to reduce cyberspace vulnerabilities and improve online privacy protections through the use of trusted digital identities by improving the ability to authenticate individuals, organizations and the underlying infrastructure involved in sensitive online transactions. According to the Frequently Asked Questions section on the NSTIC Web site,

The Identity Ecosystem is not yet built, and there are no Identity Ecosystem credentials available yet. While some private sector identity providers do exist, the technical and policy standards of the Identity Ecosystem are not yet established. The private sector, facilitated by the National Program Office at the Department of Commerce, will lead the development of these technical and policy standards. The purpose of NSTIC is to set in motion the public and private efforts that will lead to the Identity Ecosystem, but it will be many years before the full promise of the Identity Ecosystem is realized.

The National Program Office, in collaboration with the U.S. Department of Homeland Security and other federal agencies as well as the private sector, will develop the legal and policy frameworks necessary to implement the NSTIC. The implementation of the NSTIC has raised privacy concerns amid speculation that the "Identity Ecosystem" would involve the creation of a centralized database of user information.

Source: http://www.switched.com/2011/01/10/obama-drafting-internet-id-all-americans/

Source: http://www.technewsworld.com/story/71637.html?wlc=1294975503

Source: http://www.nist.gov/nstic/faqs.html

This publication is intended for educational and informational purposes only. Readers are advised to seek appropriate professional consultation before acting on any matters in this update. This report may be considered attorney advertising. To be removed from our mailing list, please email unsubscribe@pullcom.com with "Unsubscribe" in the subject line. Prior results do not guarantee a similar outcome.