The Front Burner
Cybersecurity

Office of the Chief Information Officer
Office of Cyber Security
Issue No. 15, January 2014

DOE eSCRM Program

The Department of Energy (DOE) Enterprise Supply Chain Risk Management (eSCRM) Program is an enterprise approach to managing risk and vulnerabilities associated with critical acquisition, sustainment, and disposal of information and communications technology (ICT) systems and components.

The eSCRM Program provides the Department with a robust toolset of defense-in-breadth and defense-in-depth supply chain resources to address and mitigate the evolving cybersecurity and supply chain risks. In doing so, the eSCRM Program significantly enhances the DOE enterprise's cybersecurity posture by securing the supply chain of National Security Systems (NSS).

The Department may leverage the eSCRM Program's enterprise-based capabilities to address mission-based supply chain risk issues. The program's primary SCRM capabilities include policies and procedures, as well as the Supply Chain Risk Management-Resource Center (SCRM-RC).

SCRM Policies and Procedures

DOE Order 205.1B was amended in March 2013 to incorporate supply chain risk management (SCRM) into the existing Senior DOE Management (SDMs) Risk Management Implementation Plan requirements. The Order provides considerations to assist SDMs in formulating their SCRM programs.

SCRM-RC

The SCRM-RC is a centralized Focal Point that directly supports supply chain risk-based decisions executed by SDMs and Program Managers (PMs).

The SCRM-RC provides the following capabilities:

SCRM SME

- RMIP development support to SDMs, which includes supply chain best practices, general considerations, FIPS 199 standards, and contract language.

Training, Outreach, and Awareness

- ICT SCRM Training Courses on DOE Online Learning Center and in CD format.

Supply Chain Risk Model

- The Suppy Chain Model supports SDMs or PMs by identifying the maximum acceptable risk that an agency, department, program, and / or risk owner is willing to incur and analyzes vendor risks through open source assessments, in support of risk-based decisions.

Incident Management Support

- Provide support for supply chain related incident activities (SCRM mitigation techniques, requirements for certified vendors, etc.).

Program Administration

- Collect program information from the DOE enterprise and provide reports to DOE leadership and others (Congress, GAO, IG, CNSS, DHS).

Metrics & Key Performance Indicators

- Quantity of SCRM support requests, quantity of open source intelligence reports, risk threshold determinations, quantity of customers, and impact to enterprise.

Conclusion

The eSCRM Program provides enterprise-based capabilities that the Department may leverage to address mission-based supply chain risk issues. The Program provides a significant cost savings for the Department by eliminating duplicative resourcing and its related costs, as well as providing centralized insight into enterprise-wide supply chain risks.

Secure Online Shopping

For many American consumers, online shopping has become a commonplace activity. In fact according to recent e-commerce industry statistics, approximately 167 million U.S. consumers shopped online in 2012 spending an average of $1,207 per consumer. Further, Americans spent approximately $1.45 billion last year on Cyber Monday (i.e., Monday following Thanksgiving).

There are many advantages to shopping online – at home convenience, no crowds, more variety, easy to compare prices, no pushy salesmen, etc. However, increased convenience can often have negative consequences especially when personal identity and financial information is involved. Given the sophisticated methods used by e-commerce criminals to steal consumer information, we are all accepting a certain amount of risk by purchasing products in cyberspace. But for many consumers, this risk has become better understood *and* acceptable due to the desired convenience of online shopping.

Although risks do exist, there are simple security practices that you can follow to help protect yourself.

Keep a clean machine. Make sure your software, operating system, and antivirus programs are updated. This is a critical step in the fight against viruses and malware that can be sent through emails, links, and websites.
Connect with care. Do not do online shopping on unsecure wireless networks, such as places with public and free Wi-Fi. Do your online shopping at home and password protect your home wireless network.
Pay attention to website URLs. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .net instead of .com). Also, only shop from a site that uses https://. This indicates that the company is taking extra measures to protect your information.
Set strong passwords. Make sure your passwords are complex and unique to each account. At a minimum, create passwords with eight characters or more that use a combination of numbers, letters, and symbols. Change your passwords often.
Don't believe everything you see. Always be aware of cyber scams – if it sounds too good to be true, it probably is. Only shop on trusted websites and do not follow unsolicited web links in email and pop-up ads.
Use a credit card. There are laws that limit your liability for fraudulent card charges. You may not have the same level of protection when using a debit card.
Check your statements. Regularly check your credit card and bank statements. If there are discrepancies, report them immediately.

Contributing sources to this article: U.S. Department of Homeland Security and Internet Retailer.com.

Steven Bucci to Present at Forrestal

A *Holistic* Look at CYBERSECURITY
WHY IS IT NEEDED?

Thursday, January 30, 2014
10:30 am to 12:00 pm
Forrestal Auditorium

The OCIO will host Dr. Steven Bucci, from the Douglas and Sarah Allison Center for Foreign Policy, to speak on four areas:

- The relevancy of Cybersecurity and Supply Chain Risk Management to senior leaders
- The threats we presently face
- The shift in the world that Energy operates
- The role of senior leaders in addressing these challenges

Dr. Steven Bucci is former Army Green Beret, Military Assistant to Secretary of Defense, Deputy Assistant Secretary of Defense for Homeland Defense & Defense Security Cooperation Agency, and Professor focused on Cybersecurity and the Emerging Threat. Dr. Bucci served as one of IBM's lead consultants for Cybersecurity Policy, in IBM's Public Sector Team. Dr. Bucci brings over 30 years of leadership at the highest levels of our Government in response to all security threats to America.

Please join us for this informative event. Conference Call-in number (202) 287-6172.

*For questions regarding these articles or any Cybersecurity issue, search **cybersecurity** on Powerpedia or send an e-mail to cybsectrn@hq.doe.gov.*