Department of Energy
Washington, DC 20585

September 27, 2012

JM CHRONOLOGY
JM RECEIVED 11/2/12
OUT FOR REVIEW 11/9/12
DRB DISCUSSION 11/15/12

MEMORANDUM FOR INGRID KOLB
DIRECTOR, OFFICE OF MANAGEMENT

THROUGH: KEVIN T. HAGERTY
DIRECTOR, OFFICE OF INFORMATION RESOURCES

FROM: ROBERT BRESE
CHIEF INFORMATION OFFICER
OFFICE OF THE CHIEF INFORMATION OFFICER

PAGE CHANGE TO 0205.1B WAS APPROVED BY DRB, VICE NOTICE.

DOE N 205.19

SUBJECT: Develop an Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Notice

PURPOSE: To propose a new Notice be published and implemented concerning ICT SCRM.

JUSTIFICATION: The reliance upon globally sourced information technology (IT) exposes Federal information systems to the risk of exploitation through counterfeit materials, malicious software, or untrustworthy products. In response to this evolving threat, The Department of Energy (DOE) must assess and manage supply chain risks to ensure mission success. In March 2012, the Government Accountability Office (GAO) submitted a report to Congressional requesters on ICT Supply Chain. In this report, the GAO made three recommendations:

1. Develop and document Departmental policy that defines which security measures should be employed to protect against supply chain threats;

2. Develop, document, and disseminate procedures to implement the supply chain protection security measures defined in Departmental policy and;

3. Develop and implement a monitoring capability to verify compliance with, and assess the effectiveness of, supply chain protection measures.

Publishing this Notice is a first step in institutionalizing ICT SCRM within DOE. This Notice will also provide the general direction and minimum requirements for developing and documenting processes to detect the occurrence, reduce the likelihood of occurrence, and mitigate the consequences of ICT products containing counterfeit components or malicious functions in Senior DOE Management (SDM) Risk Management Implementation Plans. The requirements specifically address components of all National Security Systems and any unclassified systems categorized as High Impact in accordance with Federal

Printed with soy ink on recycled paper

Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems.*

IMPACT: The proposed Notice will support the recommendations set forth in GAO-12-361 and address increasing supply chain issues in Departmental ICT resources for systems covered under the Federal Information Security Management Act (FISMA). This Notice addresses the risks outlined in the attached Risk Identification and Assessment to include a gap analysis of existing risks and controls as well as risk mitigation techniques. No budget impact is anticipated.

WRITER: Susan Farrand, 202-586-2514

OPI/OPI CONTACT: Mr. Gil Vega, 202-586-0166

Concur: _____ Nonconcur: _____ Date: 11-15-12

This policy/requirements will be included in the order rather than a notice. Expedited review process will be used and comments will be limited to the revised language.

Met with IM November 16, 2012 and established expedited directive development for Page Change of O 205.1B, *Department of Energy Cyber Security Program*

Draft Development	30 days
Review/Comment	30 days
Comment Resolution	30 days
Final Review	30 days

NOTE: Final review includes a collaborative process:
-Post redline/strikeout in RevCom for information purposes only
-Distribute redline/strikeout to the DRB
-Review of document by DRB members prior to meeting (a week)
-Discuss document at DRB meeting
-Prepare approval or impasse package (a week)

Risk Identification and Assessment

Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM)[1]

Risk	Probability	Impact	Risk Level
People			
1. Compromise of Personally Identifiable Information	**Likely**	**Medium**	**Significant**
2. Inability to communicate across multiple platforms (email, voice, and data)	**Possible**	**Medium**	**Acceptable**
Mission			
3. Infiltration of Sites through insertion of malicious code into software and hardware systems	**Likely**	**Medium**	**Significant**
4. Denial of Service through counterfeit ICT components	**Possible**	**Medium**	**Acceptable**
5. Mission critical function alteration or failure through malware or counterfeit.	**Likely**	**Medium**	**Significant**
6. Compromise of confidentiality, integrity, and availability of Federal information systems	**Likely**	**Medium**	**Significant**
Assets			
7. Manipulation of hardware and software baselines	**Possible**	**Medium**	**Acceptable**
8. Counterfeit components that cause premature system failure	**Possible**	**High**	**Significant**
9. Required replacement of assets prior to end of life	**Possible**	**Low**	**Acceptable**
10. Unavailability of information and information servers or services from site or Department due to issues or problems with IT Supply Chain	**Possible**	**High**	**Significant**
11. Inadequate understanding and management of the risk increase the potential for compromise of information systems and assets	**Likely**	**Medium**	**Significant**
Financial			
12. Incur costs for replacement hardware and software	**Possible**	**Low**	**Acceptable**
13. Personnel costs to support mitigation, repair and replacement of ICT systems	**Possible**	**Low**	**Acceptable**
Customer and Public Trust			
14. Loss of trust and political concern with Federal Agency partners and externally with Public	**Possible**	**High**	**Significant**
15. Lack of visibility and traceability of component viability decreases the ability to manage the risk of intentional or unintentional compromise.	**Possible**	**High**	**Significant**

[1] This analysis relates to the risks to information and information systems from failure or compromise due to vulnerabilities injected in the supply chain. This analysis does not address programmatic risks that may result from failure or compromise of mission-critical systems (e.g., release of classified information).

Gap Analysis of Existing Risks and Controls

Laws	• *P.L. 106-65, National Defense Authorization Act [Section 3212(d)], enacted October 1999* • *P.L. 107-347, Title III, Federal Information Security Management Act of 2002 (FISMA), enacted December 2002*
External Regulation	• N/A, however Defense Nuclear Facilities Safety Board will show interest in this change
DOE Regulation	•
DOE Orders	• DOE O 205.1B, Department of Energy Cyber Security Program, dated May, 16, 2011 • DOE O 206.1, Department of Energy Privacy Program, dated January, 16, 2009.
Contract Controls	• Specified in Contractor Requirement Documents (CRDs)
External Assessments	• GAO-12-361

Risk Mitigation Techniques

Risk/ Opportunity	Potential Cost/Benefit	Proposed Mitigation Technique	Specific Control(s)
(1) and (2)	Securing critical components throughout the supply chain will mitigate unintended release of PII and increase the likelihood that DOE ICT Systems remain operational. Initial cost will increase as this program	Criticality and prioritization analysis of critical components. Identification of potential threats as it relates to the components and placing specific actionable language into the procurement to ensure the vendors	The SDM RMIP is to address the following, as applicable. a. Policies and procedures to assess the criticality of systems and components to which ICT SCRM controls must apply. At a minimum, such controls must be applied to all National Security Systems and unclassified Federal information systems categorized as High Impact in accordance with Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems. b. Policies and procedures to identify and understand the risk environment, including a description of the overall (identified) risk to which the supply chain is exposed c. ICT SCRM policy and processes for the documentation, control and tracking, and approval of the provenance of information technology

Risk/ Opportunity	Potential Cost/Benefit	Proposed Mitigation Technique	Specific Control(s)
	is incorporated into the existing Risk Management Program. ROI is significant if securing the supply chain precludes the loss of PII and the interruption of ICT capability.	provide secure, not counterfeit components.	systems and assets. Policies and procedures are to reflect a risk-based defense-in-depth strategy that - includes at least the following: (1) Threat and vulnerability assessment (2) Risk Assessment and tolerance (3) Acquisition planning, sourcing, and safeguards (4) Evaluation of system component/service suppliers (5) Analysis of supplier assurance practices and due diligence to reduce supply chain risk (6) Product evaluation (7) Control of the quality, configuration, and security of software, hardware, and systems throughout their lifecycles (8) Asset management (i.e., receiving, storage, replenishment, issuing, tracking, inventory, and disposal of Government-owned property) (9) Accountability, control, visibility, protection, and identification of controlled inventory items (CII) (10) Operations Security (OPSEC) mitigation methodologies (11) Weakness/deficiency detection, reduction, and mitigation strategies (12) Incident management (13) Training and awareness (14) Monitoring and reporting d. Inclusion of IT SCRM controls in system documentation, including design and implementation plans; threat, vulnerability, and risk assessments; System Security Plans (SSPs); and Security Testing and Evaluation (ST&E) procedures, as applicable. e. Identification of roles and responsibilities for the SDM ICT SCRM program.
(3-6)	Cost incurred by mission failure. The benefit is to preclude mission failure for hardware and software systems that support mission platforms, negates denial of services to	Identify critical systems and components that need to have specific controls or procurement requirements applied. Ensure chosen vendors have the appropriate internal	Refer to specific controls in item (1)

Risk/ Opportunity	Potential Cost/Benefit	Proposed Mitigation Technique	Specific Control(s)
	critical mission systems, and ensures mission functions are not altered through counterfeit products or malicious code	controls to preclude mission failure.	
(7-11)	There will be initial cost associated with identification and procurement of secure components. This investment will provide a more secure supply chain and ultimately reduce the possibility of premature replacement of systems, lost information, and critical mission failure.	Criticality and Prioritization analysis to identify critical mission systems and the ICT components that needs to be secured. Include these requirements in the procurement. Monitoring and controls for access to the systems. (significant)	• Refer to specific controls in (1) and (2)
(12-15)	Replacement cost for systems that were damaged or destroyed by the insertion of malicious code or counterfeit parts. Benefit to securing	Criticality and Prioritization analysis to identify critical mission systems and the ICT components that needs to be secured.	Refer to specific controls in (1) and (2)

Risk/ Opportunity	Potential Cost/Benefit	Proposed Mitigation Technique	Specific Control(s)
	the supply chain for critical components is a reduced vulnerability and cost saving over the life cycle of the system.	Include these requirements in the procurement. Monitoring and controls for access to the systems. (significant)	