Department of Energy
Washington, DC 20585

JM CHRONOLOGY
JM RECEIVED 7/28/14
OUT FOR REVIEW 7/28/14
DRB DISCUSSION 8/7/14

MEMORANDUM FOR INGRID KOLB
DIRECTOR
OFFICE OF MANAGEMENT

THROUGH: KEVIN T. HAGERTY
DIRECTOR
OFFICE OF INFORMATION RESOURCES

FROM: ROBERT BRESE
SENIOR AGENCY OFFICIAL FOR INFORMATION SHARING AND SAFEGUARDING
OFFICE OF THE CHIEF INFORMATION OFFICER

SUBJECT: Notice of Intent to Develop an Information Sharing and Safeguarding Program Notice

PURPOSE: This memorandum provides justification for establishing a Directive that sets forth requirements and responsibilities for the Department of Energy's (DOE) Information Sharing and Safeguarding (ISS) Program for the responsible sharing and safeguarding of Agency information to enhance national security, protect the safety of the American people, and encourage sustained collaboration between Federal, state, local, tribal, territorial, private sector, and foreign partners.

JUSTIFICATION: Following the unlawful disclosure of classified information by WikiLeaks in the summer of 2010, President Obama signed E.O. 13587, "*Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*," which directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks. E.O. 13587 underscores that Agencies bear the primary responsibility for sharing and safeguarding classified information, consistent with appropriate protections for privacy and civil liberties. On August 22, 2013, in response to the Executive Order, Secretary Moniz designated the Chief Information Officer as the Senior Agency Official (SAO) to oversee information sharing and safeguarding efforts of the Department.

The White House considers the information sharing and safeguarding reforms as critical elements of the Government's push to improve cybersecurity and expects implementation of the first round of reforms to be complete by Calendar Year (CY16). To meet the White House "drive toward completion" time frame, DOE will need to complete the tasks by end of CY16. On June 17, the Secretary directed the SAO, with the DOE Information Sharing and Safeguarding Board (ISSGB), to develop Departmental requirements (expectations) for the implementation of information sharing and safeguarding initiatives (to be promulgated by

RECEIVED 7/28/14 C.Tirado

memorandum or Directive revision). The DOE ISSGB agreed the appropriate method to meet these White House requirements in support of the Secretary's objective was to expedite the development of a Notice. The Notice will clearly articulate roles and responsibilities, oversight/validation and particularly Departmental Elements' accountability, responsibility, and authority for implementation of the initiatives and reporting the results.

In the development of this Notice, the SAO will work with the ISSGB, as well as the Program Offices and other stakeholders to develop appropriate requirements and responsibilities. An Enterprise Risk Management (ERM) Risk Identification and Assessment has been performed, in accordance with applicable standards, and is included in this package. Within one year the Notice will be converted or incorporated into an Order.

There are no valid external, consensus, or other standards, e.g., International Organization for Standardization (ISO), etc., available that can be used in place of this Directive.

IMPACT: The proposed Notice does not duplicate existing laws, regulations, or National standards, and it does not create undue burden on the Department.

WRITER: Ms. Katherine Crouch, 202-586-2486

Office of Primary Interest (OPI)/OPI CONTACT: Mr. Robert Brese, 202-586-0166

Concur: for Ingrid Kolb Nonconcur: _____ Date: 8/7/2014

Unless determined otherwise by the Directives Review Board (DRB), writers will have up to 60 days in which to develop their first draft and submit to the Office of Information Resources, MA-90.

Standard Schedule for Directives Development	Days
Draft Development	Up to 60 days
Review and Comment (RevCom)	30
Comment Resolution	30
Final Review	30
Total	150

Note:
- NNSA Statute Language will be added in the Notice
- PGS.5 - Special nuclear material has been removed on the risk assessment.

(**NOTE**: ***The standard schedule of up to 150 days will be used unless otherwise specified by the Directives Review Board.)***

CBrese 8/7/2014

Risk The purpose is to establish a Directive that sets forth requirements and responsibilities for the Department of Energy's (DOE) Information Sharing and Safeguarding (ISS) Program for the responsible sharing and safeguarding of Agency information to enhance national security, protect the safety of the American people, and encourage sustained collaboration between Federal, state, local, tribal, territorial, private sector, and foreign partners.	Probability	Impact	Risk Level
People			
The President, under E.O. 13587, directs structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of classified information consistent with appropriate protections for privacy and civil liberties. While the Department has long had requirements that address safeguarding classified information, they do not meet comprehensively all the objectives of the Executive Order. Since there is a national level body (Senior Information Sharing and Safeguarding Steering Committee established by E.O 13587, Section 3) requiring quarterly reports on Departmental efforts to implement White house reforms, it is essential that an notice be prepared as quickly as possible to ensure Departmental compliance.	Likely	Medium	Significant
Mission			
The Department, as agency requiring classified information to perform its mission, cannot be effective in completing its mission if it is not compliant with this E.O. 13587.	Likely	High	Extreme
Assets			
Unauthorized actions such as Wikileaks involving Restricted Data, and other classified information may be overlooked, resulting in compromise or disclosure of classified information.	Unlikely	High	Significant
Financial	NA	NA	NA
Customer and Public Trust			
Failure to address E.O. requirements will reduce customer and public trust in the Department's ability to protect national security assets.	Possible	Medium	Significant

Gap Analysis of Existing Risks and Controls

Type of Control	Control	Gap Analysis
Laws	Atomic Energy Act Federal l Information Security Management Act of 2002	•

Type of Control	Control	Gap Analysis
Executive Order	E.O. 12968 E.O. 13566 E.O. 13587	• Establishes requirements for access to classified information. • The President directed agencies to give the "highest priority" to the prevention of terrorism and the "interchange of terrorism information [both] among agencies" and "between agencies and appropriate authorities of States and local governments • Establishes structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of classified information.
External Regulation	32 CFR 2004, *National Industrial Security Program* National Security Directive (NSD) 42, National Policy for the Security of National Security Telecommunications and Information Systems Presidential Policy Directive 1 National Strategy for Information Sharing and Safeguarding (NSISS).	
DOE Regulation	Secretary Moniz designates the CIO as the SAO for Information Sharing and Safeguarding, August 23, 2013	
DOE Orders	DOE O, 470.5 DOE Insider Threat Program DOE 205.1B, DOE Cyber Security Program	Addresses requirements for the DOE Insider Threat Program only. Addresses Department Cybersecurity Program. Does not include information sharing and safeguarding requirements.
Contract Controls	• None	Contractor Requirements Document (CRD) needs to be added to a new notice to establish contractor requirements.
External Assessments	• NSA as the Executive Agent	NSA provided a list of 16 departments/agencies to be assessed in the remainder of 2014 and 2015. DOE is not included in the assessment list. DOE will likely be assessed in 2016.

Risk Mitigation Techniques

[Use the risk mitigation techniques and guidance within the attached reference to fill out the chart below. List all risks that have been identified in the gap analysis. When examining the relative cost-benefit of a proposed control be careful to notice situations where a risk-specific control may also (directly or indirectly) address a separate risk identified in the gap analysis.]

Risk Assessment for DOE Information Sharing and Safeguarding Program					
Risk/Opportunity	**Risk Level**	**Potential Cost/Benefit**	**External Control(s)**	**Proposed Mitigation Technique**	**Internal Control (if needed)**
The President, under E.O. 13587, directs structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of classified information consistent with appropriate protections for privacy and civil liberties. While the Department has long had requirements that address safeguarding classified information, they do not meet comprehensively all the objectives of the Executive Order. Since there is a national level body (Senior Information Sharing and Safeguarding Steering Committee established by E.O 13587, Section 3) requiring quarterly reports on	Significant	It is of significant benefit to the Department to be in compliance with Presidential directives, especially if an insider similar to WikiLeaks or Snowden should be discovered in DOE/NNSA. Establish a unified, effective approach to DOE ISSE engaging DOE Enterprise stakeholders	E.O. 13587	Establish an Information Sharing and Safeguarding directive to coordinate and implement E.O 13587 and other national-level direction.	As mandated in the E.O. 13587 and the proposed ISS Program Notice: • There will be quarterly reporting via the KISSI reports back to the SAO and reporting to Steering committee • Quarterly reporting to the DOE Cyber Council • Annual report submitted through the Steering committee which will be reported to the President (and Congress). • Additional reporting, accountability and oversight will be defined in the Notice as well as additional reporting as determined by the

Risk Assessment for DOE Information Sharing and Safeguarding Program					
Risk/Opportunity	**Risk Level**	**Potential Cost/Benefit**	**External Control(s)**	**Proposed Mitigation Technique**	**Internal Control (if needed)**
Departmental efforts to implement White house reforms, it is essential that an notice be prepared as quickly as possible to ensure Departmental compliance.					Program Manager-Information Sharing Environment (PM-ISE).
The Department, as an agency requiring classified information to perform its mission, cannot be effective in completing its mission if it is not compliant with this E.O.	Extreme	The Department will benefit from an improved reporting on classified information. Enhance DOE's reputation as a responsible interagency partner in information Sharing and Safeguarding. Instill Cross-Department visibility/integration of KISSI and CAP Goal reporting	E.O. 13587	Establish an Information Sharing and Safeguarding directive to coordinate and implement E.O. 13587 and other national-level direction.	As mandated in the E.O. 13587 and the proposed ISS Program Notice: • There will be quarterly reporting via the KISSI reports back to the SAO and reporting to Steering committee • Quarterly reporting to the DOE Cyber Council • Annual report submitted through the Steering committee which will be reported to the President (and Congress). • Additional reporting, accountability and oversight will be defined in the Notice as well as additional reporting as determined by the Program Manager-Information Sharing Environment (PM-ISE).

Risk Assessment for DOE Information Sharing and Safeguarding Program					
Risk/Opportunity	**Risk Level**	**Potential Cost/Benefit**	**External Control(s)**	**Proposed Mitigation Technique**	**Internal Control (if needed)**
Unauthorized actions such as Wikileaks involving Restricted Data, and other classified information may be overlooked, resulting in compromise or disclosure of classified information.	Significant	The cost to national security of the disclosure of certain information to unauthorized persons is extreme, while the benefit of precursors to unauthorized actions has the potential for significant savings of staff time and effort.	E.O. 13587	Establish an Information Sharing and Safeguarding directive to coordinate and implement E.O. 13587 and other national-level direction.	As mandated in the E.O. 13587 and the proposed ISS Program Notice: • There will be quarterly reporting via the KISSI reports back to the SAO and reporting to Steering committee • Quarterly reporting to the DOE Cyber Council • Annual report submitted through the Steering committee which will be reported to the President (and Congress). • Additional reporting, accountability and oversight will be defined in the Notice as well as additional reporting as determined by the Program Manager-Information Sharing Environment (PM-ISE).
Failure to address E.O. requirements will reduce customer and public trust in the Department's ability to protect national security assets.	Significant	Both Departmental and U.S. government credibility is at risk if priority actions, 45-day measures etc. are not implemented and reporting is not	E.O. 13587	Establish an Information Sharing and Safeguarding directive to coordinate and	As mandated in the E.O. 13587 and the proposed ISS Program Notice: • There will be quarterly reporting via the KISSI reports back to the SAO and reporting to Steering

Risk Assessment for DOE Information Sharing and Safeguarding Program					
Risk/Opportunity	**Risk Level**	**Potential Cost/Benefit**	**External Control(s)**	**Proposed Mitigation Technique**	**Internal Control (if needed)**
		complete and comprehensive. Cost of remediation of DOE environment due to an event.		implement E.O. 13587 and other national-level direction.	committee • Quarterly reporting to the DOE Cyber Council • Annual report submitted through the Steering committee which will be reported to the President (and Congress). • Additional reporting, accountability and oversight will be defined in the Notice as well as additional reporting as determined by the Program Manager-Information Sharing Environment (PM-ISE).).

References

Risk/Opportunity Categories

- People – Risks that affect the individual well being.
- Mission – Risks that impede the ability of the department or offices to accomplish their mission.
- Assets – Risks that impact federal land, buildings, facilities, equipment, etc.
- Financial – Risks that may incur costs or obligations outside of DOE's control.
- Customer and Public Trust – Risks that affect the trust and political environment around DOE.

Probability Ratings

- Rare – even without controls in place, it is nearly certain that event would not occur
- Unlikely – without controls in place, it is unlikely the event would occur
- Possible – without controls in place, there is an even (50/50) probability that the event will occur
- Likely – without controls in place, the event is more likely than not to occur
- Certain – without controls in place, the event will occur

Impact Ratings

Rating	Risk	Opportunity
Negligible	Events of this type have very little short-term or long-term impact and whatever went wrong can be easily and quickly corrected with little effect on people, mission, assets, finances, or stakeholder trust.	A benefit with little or no improvement of operations or utilization of resources.
Low	Events of this type may have a moderate impact in the short term, but can be easily and quickly corrected with no long term consequences.	A benefit with minor improvement of operations or utilization of resources.
Medium	Events of this type have a significant impact in the short term and the actions needed to recover from them may take significant time and resources.	A benefit with somewhat major improvement of operations or utilization of resources.
High	Events of this type are catastrophic and result in long-term impacts that significantly affect the ability of the Department to complete its mission.	A benefit with major improvement of operations or utilization of resources.

Risk Level Ratings

		Impact			
		Negligible	Low	Medium	High
Probability	Certain	Minor	Moderate	Extreme	Extreme
	Likely	Minor	Moderate	Significant	Extreme
	Possible	Minor	Moderate	Significant	Extreme
	Unlikely	Minor	Minor	Moderate	Significant
	Rare	Minor	Minor	Minor	Moderate

Risk Mitigation Options and Guidance

- Acceptance
- Monitoring
- Mitigation
- Avoidance

Unmitigated Risk / Strategy	Extreme	Significant	Moderate	Minor
Acceptance	• Not Appropriate	• Not Appropriate	• Not Appropriate	• Risks can be handled through performance feedback and accountability
Monitoring	• Mandatory Contractor independent assessments • Federal oversight with a mandatory periodicity • Mandatory, periodic reporting	• Mandatory Contractor Self-assessments with a minimum periodicity • Federal oversight with a periodicity that is based on performance • Mandatory, periodic reporting	• Limited Federal oversight based on performance • Mandatory reporting of threshold events	• Federal oversight on a for-cause basis • Standard performance evaluation processes
Mitigation	• Federal approvals of individual transactions • Detailed performance or process requirements • Detailed design requirements	• Federal approvals of systems and programs • Detailed performance or process requirements • Detailed design requirements	• Detailed performance requirements	• General Performance Requirements
Avoidance	• Prohibition of activities or operations	• Prohibition of activities or operations	• Prohibition of activities or operations	• Guidance