Department of Energy
Washington, DC 20585

JM CHRONOLOGY
JM RECEIVED 7/31/13
OUT FOR REVIEW 8/6/13
DRB DISCUSSION 8/15/13

MEMORANDUM FOR: INGRID KOLB
DIRECTOR
OFFICE OF MANAGEMENT

THROUGH: KEVIN T. HAGERTY
DIRECTOR
OFFICE OF INFORMATION RESOURCES

FROM: GLENN S. PODONSKY
CHIEF HEALTH, SAFETY AND SECURITY OFFICER
OFFICE OF HEALTH, SAFETY AND SECURITY

SUBJECT: Notice of Intent to Develop a Department of Energy Order to Integrate Existing Technical Security Program Requirements

DOE O 470.5

PURPOSE: This memorandum provides justification for the development of one integrated and consolidated set of requirements for the Department of Energy (DOE) Technical Security Program (TSP). This Order will combine the existing necessary requirements from DOE Manual (M) 205.1-3, Telecommunications Security Manual, dated 4-17-2006 and DOE M 470.4-4A chg.1, Information Security Manual, dated 10-12-2010; Section D – Technical Surveillance Countermeasures, into a single DOE Order defining the DOE TSP.

JUSTIFICATION: The combination of the two existing DOE Manuals into a single Order is needed to ensure the TSP has current and effective policies and procedures. Many components of the existing manuals are redundant, inefficient in their execution and at times out dated. Some components of DOE M 205.1-3, Telecommunications Security Manual, no longer are synchronized with current National requirements. This directive will provide the DOE community with a cohesive implementation roadmap and structure needed to assure compliance with numerous external requirements that have been issued by multiple agencies. The combination of these parts of older DOE Manuals into a single, new directive will aid in the elimination of duplication related to our adherence to, and compliance with, national level policies, e.g. National Security Directives.

IMPACT: The proposed directive will not duplicate existing laws, regulations or national standards, and it does not create undue burden on the Department; rather it will define the DOE implementation process. No conflicts with other Directives have been identified, however, if during the development of this order conflicts are identified, applicable conforming changes will be proposed via the revision process. Negative impacts to current Departmental functions or operations are not anticipated and we have purposely included all locations having TSP interests in the order development process so that any issues that would be identified can be resolved during the writing stage of the process. There are minimal expectations of any increase in costs associated with the implementation of the new combined order. Most, if any, cost increases are

likely to be completely offset by savings associated with the resulting, streamlined operations and the resultant reduction in risk to DOE assets.

WRITER: Sam Soley, HS-1.2, (301) 903-9992. The draft is being written by several working groups consisting of representatives from the TSP community DOE-wide. Separate working groups have been established for the following topical areas: Technical Surveillance Countermeasures, cyber security, TEMPEST, COMSEC and physical security. When each working group completes their section, an overarching committee will finalize the integrated draft Order.

OPI/OPI CONTACT: Sam Soley, HS-1.2, (301) 903-9992

Decision: Ingrid Kolb, Director, Office of Management (MA-1):

Concur: Nonconcur: Date: 8-21-13

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

Risk Identification and Assessment

Risk	Probability	Impact	Risk Level
People			
1. Without this action, any resulting disclosure of classified or sensitive information from DOE resources could place DOE personnel and the US public at risk of physical harm.	**Unlikely**	**Medium**	**Moderate**
Mission			
2. Failure to update and combine the existing Manuals into the single Order will result in DOE failing to comply with standards established by external Federal agencies such as National Institute for Science and Technology (NIST) and Committee on National Security Systems (CNSS).	**Certain**	**Medium**	**Extreme**
3. Failure to comply with existing ODNI policy could result in revocation of DOE's SCIF accreditation authority.	**Likely**	**High**	**Extreme**
Assets			
4. If TSP operations are compromised, classified and/or sensitive information may be intercepted or compromised.	**Certain**	**High**	**Extreme**
Financial			
5. Potential loss of contracts due to loss of reciprocity with other federal agencies regarding DOE's operating environment.	**Likely**	**High**	**Extreme**
6. A single DOE Order would help ensure all sites operate in a uniformed consistent manner and assist in eliminating operational duplicity, providing a qualitative benefit.	**Likely**	**Medium**	**Significant**
Customer and Public Trust			
7. Public trust could be lost or irreversibly damaged in the event of a compromise of classified and/or sensitive information.	**Likely**	**High**	**Extreme**
8. Trust within DOE and between DOE and other agencies could waiver if operational shortfalls occur.	**Likely**	**High**	**Extreme**
9. Community trust could be adversely affected if DOE policies and procedure fail to comply fully with National standards.	**Likely**	**High**	**Extreme**

Gap Analysis of Existing Risks and Controls

Laws	• See attached listing
External Regulation (core listing—see attachment for comprehensive listing)	• 32 Code of Federal Regulation Part 149, Policy on Technical Surveillance Countermeasures (DoD) • National Institute of Standards and Technology Guidelines on Cell Phone and PDA Security, Special Publication 800-124 • Office of The Director of National Intelligence (ODNI) Intelligence Community Baseline Requirements for Converged Devices (aka Portable Electronic Devices (PEDs)) 1 August 2007 • ODNI Community Standard Number 2008-500-1. Application of Multi-Use and/or Keyboard, Video, and Mouse (KVM) Switches on Intelligence Community Systems. ICS 2008-500-1 • Information Systems Security Organization Information Assurance Advisory No. IAA-001-2000, Security Guidance for Using Computers with Internal Microphones • Interagency Security Committee Standard, Physical Security Criteria for Federal Buildings, April 2010Office of the National Counterintelligence Executive, IC Tech Spec-for ICD/ICS 705, Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, April 23, 2012 • American Society For Testing and Materials (ASTM) Standard Test Method of for Measurement of Airborne Sound Insulation in Buildings. Designation: E 336-97 • Security Policy Board (SPB) Issuance 6-97, National TSCM Policy • Intelligence Community Directive Number 702, Technical Surveillance Countermeasures, effective February 18, 2008 • National Policy on Security Voice Communications, NSTISSP No. 101, 14 September 1999 • National Security Telecommunications and Information Systems Security Procedures for TEMPEST Zoning. NSTISSAM TEMPEST/2-92, 30 December 1992 • Department of Defense Instruction Number 5240.05, February 22, 2006, Technical Surveillance Countermeasures (TSCM) Program • Department of the Army Regulation 380-27, Control of Compromising Emanations. 19 May 2010. • National Security Agency/Central Security Service, Information Assurance Directorate, CGS Physical Enterprise Monitoring Capability, dated July 30, 2012.
DOE Regulation	• Title 10 CFR, Energy, Parts 725, 824, 1016, 1017, 1044, 1045, and 1046
DOE Orders	• DOE M 205.1-3, Telecommunications Security Manual • DOE M 470.4-4A, Chg 1, Information Security Manual, Section D – Technical Surveillance Countermeasures
Other DOE documents	• TSCM Officer Handbook • NNSA Policy Letter, NAP 70.4, Section D dated 7-2-2010, Information Security, Section D
External Assessments	• None

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 cast-benefit of a praposed control be careful to natice situations where a risk-specific control may also (directly or indirectly) address a separate risk identified in the gap analysis.]

Risk Assessment for [Directive Number, *Directive Title*]					
Risk/Opportunity	**Risk Level**	**Potential Cost/Benefit**	**External Control(s)**	**Proposed Mitigation Technique**	**Internal Control (if needed)**
This order will identify potential hazards that could lead to unauthorized disclosure of classified information. Without this action, any resulting disclosure of classified or sensitive information from DOE resources could place DOE personnel and the U.S. public at risk of physical harm.	Moderate	Damage to the national security	Committee on National Security Systems (CNSS); National Security Agency audits and inspections; National Counterintelligence Executive (NCIX) reviews and evaluations	Consolidation of out of date manual content into one cohesive order	
Failure to update and combine the existing Manuals into the single Order will result in a failure to comply with national standards. As an example, failure to meet ODNI standards for SCIFs would result in DOE losing its accreditation authority for its SCIFse	Extreme	Mission impacts	Committee on National Security Systems (CNSS); National Security Agency audits and inspections; National Counterintelligence Executive (NCIX)	Consolidation of out of date manual content into one cohesive order	

			reviews and evaluations		
Failure to comply with existing National level policy could result in revocation of DOE's operational authority and denied reciprocity from other Federal agencies.	Extreme	Mission impacts	Committee on National Security Systems (CNSS); National Security Agency audits and inspections; National Counterintelligence Executive (NCIX) reviews and evaluations	Consolidation of out of date manual content into one cohesive order	
If TSP operations are compromised, classified and/or sensitive information may be intercepted or compromised.	Extreme	Damage to the national security	Committee on National Security Systems (CNSS); National Security Agency audits and inspections; National Counterintelligence Executive (NCIX) reviews and evaluations	Consolidation of out of date manual content into one cohesive order	
Potential loss of contracts due to loss of reciprocity with other federal agencies regarding DOE's operating environment.	Extreme	Mission impacts	Committee on National Security Systems (CNSS); National Security Agency audits and	Consolidation of out of date manual content into one cohesive	

			inspections; National Counterintelligence Executive (NCIX) reviews and evaluations	order	
A single DOE Order would better enable all sites operate in a uniformed consistent manner and assist in eliminating operational duplicity.	Significant	Mission impacts/avoidance of excessive costs at DOE sites	Committee on National Security Systems (CNSS); National Security Agency audits and inspections; National Counterintelligence Executive (NCIX) reviews and evaluations	Consolidation of out of date manual content into one cohesive order	
Public trust could be lost or irreversibly damaged in the event of a loss of classified and/or sensitive information.	Extreme	Mission impacts	Committee on National Security Systems (CNSS); National Security Agency audits and inspections; National Counterintelligence Executive (NCIX) reviews and evaluations	Consolidation of out of date manual content into one cohesive order	
Trust from within DOE divisions could waiver if operational shortfalls occur.	Extreme	Mission impacts	Committee on National Security Systems (CNSS);	Consolidation of out of date manual	

			National Security Agency audits and inspections; National Counterintelligence Executive (NCIX) reviews and evaluations	content into one cohesive order
Community trust could be adversely affected if DOE policies and procedure fail to comply fully with higher level procedural guidance.	Extreme	Mission impacts/increased cost to DOE missions	Committee on National Security Systems (CNSS); National Security Agency audits and inspections; National Counterintelligence Executive (NCIX) reviews and evaluations	Consolidation of out of date manual content into one cohesive order

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			
Probability		Negligible	Low	Medium	High
	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