National Nuclear Security Administration

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

MEMORANDUM FOR ROBERT J. NASSIF
ACTING ASSOCIATE ADMINISTRATOR
FOR MANAGEMENT AND BUDGET

THROUGH: INGRID A. KOLB
DIRECTOR, OFFICE OF MANAGEMENT

FROM: for DONALD L. COOK
DEPUTY ADMINISTRATOR
FOR DEFENSE PROGRAMS

SUBJECT: Notice of Intent to Revise DOE O 452.4B, *Security and Control of Nuclear Explosives and Nuclear Weapons*, dated 1-11-2010

ISSUE: Whether to approve the revision of the Department of Energy (DOE) Order 452.4B, *Security and Control of Nuclear Explosives and Nuclear Weapons*, dated 1-11-2010.

BACKGROUND: The current version of DOE O 452.4B, *Security and Use Control of Nuclear Explosives and Nuclear Weapons,* provides policies and responsibilities to ensure authorized use of nuclear weapons when directed by National Command Authority and protects against Deliberate Unauthorized Acts (DUAs) and Deliberate Unauthorized Use (DUU). This revision strengthens our measures by formally recognizing actions to prevent Denial of Authorized Use (DAU). The DAU measures formally acknowledge that the Department ensures that the weapon system, its components, all related support systems and processes, the nuclear weapon supply chain, and cyber security systems associated with development, production, storage, and maintenance are not subverted or compromised. DAU is a real and documented threat.

In addition to the overarching Use Control efforts that currently include DUA and DUU, the revised Order will establish a hierarchy of DAU programs and activities. The Nuclear Enterprise Assurance (NEA) Program will implement all Weapon Trust Assurance (WTA) activities to prevent DAU. The NEA will be guided by a Steering Group established and chaired by National Nuclear Security Administration (NNSA) Defense Programs senior management. The WTA activities will ensure that our weapon systems are protected from emerging threats that seek to insert components, data, or software with malicious content that can cause a nuclear weapon to not perform as designed or project doubt about the designed performance of the weapon.

Countering this recently documented threat will also require the cooperation of the DOE Chief Information Officer (CIO), the DOE Director of Intelligence and

Counterintelligence (IN), and the NNSA Associate Administrator for Information Management who are exempted from the current Order. They will need to provide information on the security of software, data, and intelligence regarding emerging threats.

Justification

Recent events have revealed that there are organizations that are seeking to insert malicious software and/or components into the nuclear weapon supply chain that can alter the functionality of the weapon and possibly cause DAU. The existence of these threats is well understood, and numerous national and Department of Defense (DoD) directives have been issued that acknowledge and counter this threat: National Institute of Standards and Technology Interagency Report (NISTIR) 7622, *National Supply Chain Risk Management for Federal Information Systems;* Committee on National Security Systems Directive (CNSSD) 505, *Supply Chain Risk Management;* DoD 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks.* Within the Department and NNSA, DOE O 205.1B, *Department of Energy Cyber Security Program*, dated 5-16-2011; DOE O 414.1D, *Quality Assurance*, dated 4-25-11; and NNSA Policy Letter (NAP) 24, *Weapon Quality Policy*, dated 6-20-13, provide policy to address the integrity of the supply chain. The need to protect against emerging threats to critical components and information that can result in DAU must be provided in a revision to this Order. These DAU threats require additional and more rigorous measures in addition to the current efforts to secure our supply chain and information systems.

NNSA, Sandia National Laboratories (SNL), and Kansas City Plant (KCP) have been developing stronger countermeasures and greater cooperation to defend against emerging threats. The revisions to this document will serve to direct and institutionalize these protections within the Nuclear Security Enterprise.

Summary of Development Process

NNSA Office of Nuclear Weapon Surety and Quality (NA-121) will coordinate with the appropriate program offices, SNL, KCP, and other stakeholders to develop the appropriate language.

In the development of the revision, NA-121 will also work with the CIO and IN and the Office of the Chief Information Officer (CIOO) to jointly develop sound practices that are achievable with the budget parameters.

A cross-functional workgroup will be tasked to assure that measures are robust and complete.

Major Changes

This revision strengthens our measures by formally recognizing actions to prevent DAU by establishing the NEA Program which will implement all WTA activities to prevent DAU under the guidance of the NEA Steering Group.

To acknowledge the efforts already in progress by the CIOO and IN and to provide the opportunity for cooperation in this area, their exemptions from this order will be removed. There are no valid external, consensus, or other "Standards (e.g., ISO, VPP) available which can be used in place of this directive.

No conflicts with other directives have been identified. No additional funds will be required.

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

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

OPTIONS: None.

RECOMMENDATION: That you approve the revision of DOE O 452.4B, *Security and Use Control of Nuclear Explosives and Nuclear Weapons.*

Ingrid Kolb, Director, Office of Management (MA-1):
Concur: ______ for Ingrid Kolb Nonconcur: ______ Date: 9/18/2014

Robert Nassif, Acting Associate Administrator for Management and Budget (NA-MB-1):
Concur: ______ Nonconcur: ______ Date: 9/18/14

Risk Identification and Assessment

Proposed Revisions to DOE452.4B -Use Controls

Risk	Probability	Impact	Risk Level
People			
1. None / Not Applicable			
Mission			
1. Current DOE/NNSA policy does not adequately cover measures to prevent DAU from occurring.	**Possible**	**High**	**Extreme**
2. Critical information is not being shared because the OCIO and IN/CI are excluded from the current Order.	**Likely**	**High**	**Extreme**
3. The National Mission of Nuclear Deterrence will fail if DAU is not prevented	**Possible**	**High**	**Extreme**
Assets			
1. Critical components and information can be compromised without stronger measures to secure the Nuclear Weapon (NW) supply chain, which can result in the subversion of weapon functionality.	**Possible**	**High**	**Extreme**
Financial			
1. National Nuclear Deterrent assets could be rendered useless if NW Systems are compromised by components with malicious content; production delays/stoppages, rework, confidence level(real or implied)additional testing are likely scenarios in the case of a breach.	**Likely**	**Medium**	**Significant**
Customer and Public Trust			
1. A NW may not function as designed or confidence can be lost that it will function in the case of a breach. The public and US officials consider this trust to be an essential deterrent.	**Likely**	**Medium**	**Significant**

Gap Analysis of Existing Risks and Controls

[Identify all controls that currently exist, excluding controls developed within this subsystem. Add more categories as necessary.]

Laws	• National Defense Authorization Act (NDAA) for FY2013, Section 833
External Regulation	• National Institute of Standards and Technology Interagency Report (NISTIR) 7622, *National Supply Chain Risk Management for Federal Information Systems* • Committee on National Security Systems Directive (CNSSD) 505, *Supply Chain Risk Management* • DoD 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks*
DOE Regulation	• None
DOE Orders	• DOE O 205.1B, *Department of Energy Cyber Security Program*, dated 5-16-2011 • DOE O 414.1D, *Quality Assurance*, dated 4-25-11 • NNSA Policy Letter (NAP) 24, *Weapon Quality Policy,* dated 6-20-13
Contract Controls	• Assistant Deputy Administrator for Stockpile Management Memorandum, *Nuclear Enterprise Assurance*, dated 9-23-2011
External Assessments	• GAO-12-361, *IT Supply Chain National; Security-Related Agencies Need to Better Address Risks*

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 DOE452.4B -Use Controls					
Risk/Opportunity	**Risk Level**	**Potential Cost/Benefit**	**External Control(s)**	**Proposed Mitigation Technique**	**Internal Control (if needed)**
Current policy does not adequately cover measures to prevent DAU from occurring.	Extreme	Cost avoidance of disruptions in the supply chain, production or in the stockpile with measures to keep malicious components from getting into the supply chain.	Processes will be assessed and gap analysis conducted. Processes will be monitored bi-annually.	Mitigation	Establish Nuclear Enterprise Assurance (NEA) Program
Critical information is not being shared because the OCIO and IN/CI are excluded from the current Order.	Extreme	Information systems are secured, protecting classified data and service disruptions are avoided	Audits for compliance to applicable NIST standards.	Mitigation	Revise DOE O 452.4B to parallel policy contained in DOE O 205.1D and work in coordination with OCIO and IN/CI
The National Mission of Nuclear Deterrence will fail if DAU is not prevented	Extreme	Cost of compromised nuclear deterrent is very high. Rework of compromised weapons and sub-systems is time-consuming and costly.	Processes will be assessed and gap analysis conducted. Processes will be monitored bi-annually	Mitigation	Establish Nuclear Enterprise Assurance (NEA) Program
Critical components and information can be compromised without stronger measures to	Extreme	Cost avoidance of disruptions in the supply chain, production or in the stockpile with measures to keep malicious	Audits and monitoring will occur to determine whether risks or compromise of the	Mitigation	Field office audits

secure the Nuclear Weapon (NW) supply chain, which can result in the subversion of weapon functionality.		components from getting into the supply chain.	components and information specified in the Program Protection Plan is adequately mitigated.		
National Nuclear Deterrent assets could be rendered useless if NW Systems are compromised by components with malicious content; production delays/stoppages, rework, confidence level (real or implied) additional testing are likely scenarios in the case of a breach.	Significant	Cost of compromised nuclear deterrent is very high. Rework of compromised weapons and sub-systems is time-consuming and costly.	Processes will be assessed and gap analysis conducted. Processes will be monitored bi-annually.	Mitigation	Establish Nuclear Enterprise Assurance (NEA) Program
A NW may not function as designed or confidence can be lost that it will function in the case of a breach. The public and US officials consider this trust to be an essential deterrent.	Significant	Cost of compromised nuclear deterrent is very high. Rework of compromised weapons and sub-systems is time-consuming and costly.	Processes will be assessed and gap analysis conducted. Processes will be monitored bi-annually.	Mitigation	Establish Nuclear Enterprise Assurance (NEA) Program

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