

U.S. Department of Energy
Washington, D.C.

MINOR CHANGE

DOE O 470.4B

Approved: 7-21-2011
Chg 1 (AdminChg): 2-15-2013
Chg 2 (MinChg): 1-17-2017

SUBJECT: MINOR CHANGE TO DOE O 470.4B, *Safeguards and Security Program*

1. EXPLANATION OF CHANGES. The Order has been updated to reflect changes in the Departmental management structure and to incorporate the Secretary-approved 2014 *Strategy of Reforms to Enhance Security, Independent Assessments, and Safety and Health Functions*. The reform includes the establishment of the positions of Chief Security Officer in the office of the Under Secretaries and the establishment of a Security Committee which is charged with developing corporate security strategies and enterprise-wide policies. These new security strategy impacted directly on the responsibilities covered in DOE O 470.4B, necessitating a minor change to incorporate the changes to the Order. Additionally, administrative changes were made to affect organizational updates as necessary in the Order's Appendices and Attachments, to update references and internet links, and to clarify existing requirements where the necessity for such changes has been brought to the attention of the Office of Primary Interest. The changes are shown in the following table.

2. LOCATIONS OF CHANGES:

Page	Paragraph	Changed	To
1	2.	DOE O 470.4A, administrative change 1, Safeguards and Security Program, dated 5-25-07; DOE M 470.4-1 Chg 2, Safeguards and Security Program Planning and Management, dated 10-20-10; and DOE O 142.1, Classified Visits Involving Foreign Nationals, dated 1-13-04.	DOE O 470.4B, administrative change 1, Safeguards and Security Program, dated 7-21-11.
2	3.c	Equivalencies/Exemptions for DOE O 470.4B	Equivalencies/Exemptions for DOE O 470.4B, Chg 2
3	4.c	The DOE Tactical Doctrine (Attachment 4) must be applied at facilities/sites. . .	The DOE Tactical Doctrine (Attachment 4) must be applied at fixed facilities/sites. . .

Page	Paragraph	Changed	To
4	5.b.(4)	Establishes the Department-wide base Security Conditions (SECON) level in consultation with the Under Secretaries; the Director, Office of Intelligence and Counterintelligence; and the Chief Health, Safety, and Security.	Establishes the Department-wide base Security Conditions (SECON) level in consultation with the Under Secretaries; the Deputy Under Secretary for Counterterrorism and Counterproliferation; the Director, Office of Intelligence and Counterintelligence; the Associate Under Secretary for Environment, Health, Safety and Security; and the Chief Security Officers.
5	5.b.(6)	Approves and issues the <i>Graded Security Protection (GSP) Policy</i> .	Approves and issues the <i>Design Basis Threat (DBT) Policy</i> . NOTE: DOE O 470.3C Design Basis Threat replaced DOE O 470.3B Graded Security Protection Policy and is reflected throughout the entirety of the document.
5	5.b.(7)	[Added additional responsibility]	Reviews and approves enhancements to Secretarial security policies identified by the Security Committee.
5	5.b.(8)	[Added additional responsibility]	Appoints the Chair of the Security Committee, comprised of the Chief Security Officers from each Under Secretarial organization and other Departmental Federal leadership.
5	5.b.(9)	[Added additional responsibility]	Approves site/facility management recommended deviation to lower from established Departmental SECON level.
5	5.b.(10)	[Added additional responsibility]	Serves as chairman, or appoints a chairman, for the Senior SECON Decision Team.

Page	Paragraph	Changed	To
6	5.c.(1)	Responsible for the management and implementation of S&S programs administered by NNSA and the Offices of Environmental Management (EM) and Legacy Management (LM).	Responsible for the management and implementation of S&S programs administered by NNSA and its subordinate offices, including provision of the appropriate level of authorities and resources to the NNSA Chief Security Officer to effectively manage and execute S&S responsibilities.
6	5.c.(2)	Authorizes continuing operations of NNSA, EM, and LM facilities/activities determined to be of moderate security risk.	Authorizes continuing operations of NNSA facilities/activities determined to be of moderate security risk.
6	5.c.(3)	In coordination with the Under Secretaries, the Office of Intelligence and Counterintelligence, and the Chief Health, Safety and Security Officer, provides recommendations on SECON levels to the Deputy Secretary.	In coordination with the Under Secretaries for Science and Energy and Management and Performance, the Director, Office of Intelligence and Counterintelligence, the Deputy Under Secretary for Counterterrorism and Counterproliferation, the Associate Under Secretary for Environment, Health, Safety and Security, and the Chief Security Officers, provides recommendations on SECON levels to the Deputy Secretary.
6	5.c.(4)	Through the Associate Administrator for Emergency Operations, monitors the SECON level for the Department and for all DOE facilities and sites.	Through the Associate Administrator for Emergency Operations, monitors the SECON level for the Department and for all DOE facilities and sites and advises DOE/NNSA officials of changes to the levels.
6	5.c.(5)(c)	Delegates in writing to a senior Federal official at each site under NNSA cognizance (5)(b) above the authority to make...	Delegates in writing to a senior Federal official at each site under (5)(b) above the authority to make...

Page	Paragraph	Changed	To
7	5.c.(8)(a)	Serves as the DOE cognizant security officer responsible for the development and implementation of security programs, operations, and facilities under the purview of NNSA.	Serves as the NNSA Chief Security Officer responsible for the development and implementation of security programs, operations, and facilities under the purview of NNSA; exercises all responsibilities of a Chief Security Officer under this Order.
7	5.c.(8)(b)	Delegates authority to serve as the cognizant security office in writing as appropriate to subordinate NNSA line managers; delegations must be reflected in the affected facility/site security plans.	Oversees implementation of SECON levels for operations under the cognizance of NNSA.
7	5.c.(8)(c)	Issues direction for and oversees implementation of SECON levels for operations under the cognizance of NNSA.	Acts as senior NNSA official responsible for the direction and administration of the NNSA implementation and compliance with the National Industrial Security Program.
7	5.c.(8)(d)	Acts as senior NNSA official responsible for the direction and administration of the NNSA implementation and compliance with the National Industrial Security Program.	Provides resources for conducting inquiries and damage assessments and for implementing corrective actions in incidents of security concern occurring at NNSA sites/facilities.

Page	Paragraph	Changed	To
7	5.c.(8)(e)	Establishes procedures for reporting incidents of security concern, and provides resources for conducting inquiries and damage assessments and for implementing corrective actions.	Acts as the senior NNSA official responsible for all classified visits except for those assigned in paragraph 5.d.(5)(b) above to the Deputy Administrator for Defense Programs; delegates in writing to a senior Federal official at each site under NNSA cognizance the authority to make, in connection with such classified visits, an affirmative determination that permitting a U.S. citizen holding a clearance granted by another Federal agency to have access to Restricted Data will not endanger the common defense and security prior to granting such access in connection with a specific classified visit.
7	5.c.(8)(f)	Directs the implementation of S&S programs in accordance with the requirements of this Order, including development of procedures and guidance on how to apply the requirements of the Order and its appendices and attachments at NNSA facilities and sites.	Implements the DOE North Atlantic Treaty Organization (NATO) program for DOE and NNSA including access authorizations, policy, operations of the DOE Sub-Registry, and the conduct of DOE domestic inspections.
7	5.d.(1-7)	[Merged responsibilities]	Under Secretary for Science and Energy...
8	5.e.(1-7)	[Added new and additional responsibilities]	Under Secretary for Management and Performance...
10	5.e.(8)	[Added new and additional responsibilities]	Through the Assistant Secretary for Environmental Management...

Page	Paragraph	Changed	To
10	5.f.(5)	[Added additional responsibility]	When new DOE S&S directives are issued, oversee the development of and approve an implementation plan describing the steps and milestone dates that will lead to full implementation of new requirements and incorporation of CRDs into affected contracts.
11	5.f.(15)	[Added additional responsibility]	Assesses the impact/potential impact (e.g., reduced operations, additional protective force or security personnel, searches, entry/exit screening, patrols, training, etc.) in response to elevated SECON level.
12	5.f.(16, a-c)	[Added additional responsibility]	Establishes higher local SECON level at their respective site/facility; or to recommend a deviation to lower from the Departmental SECON upon notification to and approval by the Deputy Secretary.
13	5.f.(17)	[Added additional responsibility]	Review/update SECON response plans, as deemed appropriate.
13	5.f.(18)	[Added additional responsibility]	Issues direction for, and oversees implementation of SECON level for sites/facilities or operations under their cognizance.
13	5.g.(1-5)	[Added new responsibilities]	Director, Office of Enterprise Assessments...
14	5.h.(1-5)	[Added new and additional responsibilities]	Chief Security Officers for NNSA, Science and Energy, and Management and Performance...
14	5.i.(1)	...HSS...	...AU...

Page	Paragraph	Changed	To
15	5.i.(6)	In coordination with the Under Secretaries, the NNSA Administrator, and the Office of Intelligence and Counterintelligence, provides recommendations on SECON levels to the Deputy Secretary.	In coordination with the Under Secretaries, the NNSA Administrator, the Deputy Under Secretary for Counterterrorism and Counterproliferation, the Associate Under Secretary for Environment, Health, Safety and Security, and the Chief Security Officers, provides recommendations on SECON levels to the Deputy Secretary.
15	5.h.(1)	[Added new and additional responsibilities]	Deputy Under Secretary for Counterterrorism and Counterproliferation...
15	5.k.	...HSS...	...AU...
16	5.n.(1-4)	[Added new responsibilities]	Senior SECON Decision Team...
16	6.	... https://pir.labworks.org/ https://pir.doe.gov .
	6.l	[Added new reference]	DOE O 227.1A, Independent Oversight Program, dated 12-21-15.
18	6.m	DOE O 414.1D	DOE O 414.1D, admin. chg 1
18	6.n	DOE O 475.2A	DOE O 475.2B
18	6.p	DOE O 243.1A, <i>Records Management Program</i> , dated 11-7-11	DOE O 243.1B, admin. change 1, <i>Records Management Program</i> , dated 03-11-13
18	6.q	Homeland Security Presidential Directive-7, <i>Critical Infrastructure Identification, Prioritization, and Protection</i> , dated 12-17-03, which establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.	Presidential Policy Directive (PPD)-21, <i>Critical Infrastructure Security and Resilience</i> , dated 2-12-13, which establishes a national policy advancing a unified effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.
18	6.s	[Added new reference]	PPD-7, National Terrorism Advisory System, dated 01-26-11.

Page	Paragraph	Changed	To
18	6.t	[Added new reference]	E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, dated October 7, 2011.
18	6.u	[Added new reference]	Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, dated November 12, 2012.
18	6.v	[Added new reference]	DOE Order 470.5, Insider Threat Program, dated June 2, 2014.
19	7.b	[Added definition]	Officially Designated Federal Security Authority (ODFSA) are Federal employees who possess the appropriate knowledge and responsibilities for each situation to which they are assigned through delegation...
19	7.c	[Added definition]	Officially Designated Security Authority (ODSA) are Federal or contractor employees that possess the appropriate knowledge and responsibilities for each situation to which they are assigned through delegation...

Page	Paragraph	Changed	To
19	7.d.	[Added definition]	Chief Security Officer is the designated Under Secretarial official responsible and accountable for the implementation of the safeguards and security programs for personnel, facilities, and sites within their respective Offices. The Under Secretaries will provide their respective Chief Security Officer the appropriate level of authorities and resources to manage and execute the significant safeguards and security responsibilities being entrusted to them.
19	7.e.	[Added definition]	Security Committee is a forum comprised of CSOs from each of the three Under Secretarial organizations, and other Departmental Federal employee leadership that participate in developing recommendations regarding Department-wide security policies, facilitate active coordination of effective security strategies across the Department, and provide a forum for addressing cross-organizational issues and challenges.
20	7.f.	. . . https://pir.labworks.org/ https://pir.doe.gov .
20	8.	. . . Office of Health, Safety and Security. Office of Environment, Health, Safety and Security. . . [Writer's Note: this change and the corresponding change from "HSS" to "AU" have been made throughout the document wherever the office name or symbol appears.]

Page	Paragraph	Changed	To
App. A, Sect. 1, 1-2	4.e	... , <i>Physical Security Criteria for Federal Facilities</i> , August 2013/1 st Edition, <i>Risk Management Process</i> .
App. A, Sect. 1, 1-2	4.f.	ISC Standard, <i>Facility Security Level Determination for Federal Facilities</i> .	Cancelled reference removed and subsequent sub-paragraphs re-lettered.
App. A, Sect. 1, 1-2	4.g.	ISC Report, <i>The Design Basis Threat (DBT)</i> .	ISC Guide, <i>Design Basis Threat</i> , September 2014/9 th Edition
App. A, Sect. 1, 1-2	4.j	HSPD-3, <i>Homeland Security Advisory System</i>	PPD-7, <i>National Terrorism Advisory System</i>
App. A, Section 1, 1-2	4.k	DOE O 150.1., <i>Continuity Programs</i> , dated 5-8-08	DOE O 150.1A, <i>Continuity Programs</i> , dated 3-31-14
App. A, Section 1, 1-2	4.l	HSPD-7, <i>Critical Infrastructure Identification, Prioritization, and Protection</i>	PPD-21, <i>Critical Infrastructure Security and Resilience</i>
App. A, Section 1, 1-2	4.m	[Added reference]	E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, dated October 7, 2011.
App. A, Section 1, 1-2	4.n	[Added reference]	Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, dated November 12, 2012.
App. A, Section 1, 1-2	4.o	[Added reference]	DOE Order 470.5, Insider Threat Program, dated June 2, 2014.

Page	Paragraph	Changed	To
App. A, Section 1, 1-2	5.	DOE cognizant security offices, as designated by the Program Secretarial Office, or for NNSA, the Office of the Administrator through the Chief, Defense Nuclear Security, . . .	DOE cognizant security offices, as designated by the Program Secretarial Office, or for NNSA, the Office of the Administrator through the Chief, Defense Nuclear Security,. . . [Writer's Note: this change has been made to the Requirements paragraph of each Section of the Order in Appendices A and B.]
App. A, Section 1, 1-2	5.c	Ensure that designated Federal approval officials. . .	Ensure that Officially Designated Federal Security Authority (ODFSA) approval officials. . .

Page	Paragraph	Changed	To
App. A, Section 1, Chap. II, II-1	1.	DOE SECON levels reflect a multitude of conditions that may adversely impact Departmental and/or facility and site security. SECONs may include terrorist activity, continuity conditions, environmental (fire, chemical, radiological, etc.) and/or severe weather conditions. The day-to-day DOE security readiness state is informed by the Homeland Security National Terrorism Advisory System (NTAS). NTAS alerts are established based on the analysis of a continuous and timely flow of integrated, all-source threat assessments and reporting provided to Executive Branch decision-makers. This chapter details DOE requirements for responding to changes in the NTAS alerts and the Departmental SECON levels.	<p>DOE Security Condition (SECON) levels reflect a multitude of conditions that may adversely impact Departmental and/or facility and site security. SECONs may include terrorist activity, continuity conditions, environmental (fire, chemical, radiological, etc.) and/or severe weather conditions. The day-to-day DOE security readiness state is informed by the Department of Homeland Security's (DHS) NTAS. NTAS alerts are established based on the analysis of a continuous and timely flow of integrated, all-source threat assessments and reporting provided to Executive Branch decision-makers.</p> <p>The SECON will be managed by a Senior SECON Decision Team, chaired by the Deputy Secretary, with membership comprised of the Under Secretaries, the Deputy Under Secretary for Counterterrorism and Counterproliferation, the Associate Under Secretary for Environment, Health, Safety and Security, the Director, Office of Intelligence and Counterintelligence and Chief Security Officers. This chapter details DOE requirements for responding to changes in the Departmental SECON levels and NTAS alerts.</p>
App. A, Section 1, Chap. II, II-1	1.	Homeland Security National Terrorism Advisory System (NTAS).	NTAS

Page	Paragraph	Changed	To
App. A, Section 1, Chap. II, II-1	1.	[Added language]	The SECON will be managed by a Senior SECON Decision Team, chaired by the Deputy Secretary, with membership comprised of the Under Secretaries, the Deputy Under Secretary for Counterterrorism and Counterproliferation, the Associate Under Secretary for Environment, Health, Safety and Security, and the Director, of Office of Intelligence and Counterintelligence and Chief Security Officers.
App. A, Section 1, Chap. II, II-1	2.(a)	[Added language]	Departmental SECON Level. Department-wide SECON levels are established by...
App. A, Section 1, Chap. II, II-1	2.(b)	[Added language]	Local SECON Levels. Local SECON levels may differ from the Departmental SECON level and are established by site/facility management with the concurrence of the cognizant Under Secretary or, in the case of DOE Headquarters, the Associate Under Secretary for Chief Environment, Health, Safety, and Security.
App. A, Section 1, Chap. II, II-1	2.(b).1	[Added language]	Elevated. If the determination is made to elevate a site/facility SECON level from the Departmental SECON...
App. A, Section 1, Chap. II, II-2	2.(b).2	[Added language]	Lowered. If the determination is made to lower a site/facility SECON level from the Departmental SECON...

Page	Paragraph	Changed	To
App. A, Section 1, Chap. II, II-2	2.(b).Table 1.	[Added table]	Table 1. Relationship of Notification System Levels.
App. A, Section 1, Chap. II, II-2	3.	[Added language]	SECON LEVELS. DOE has five SECON levels with SECON 5 being the lowest level of readiness and SECON 1 the highest...
App. A, Section 1, Chap. II, II-3	4.	[Modified language]	SECON RESPONSE PLANNING. Contractor and Federal cognizant security offices must develop SECON response plans that...
App. A, Section 1, Chap. II, II-4	5.	[Added language]	PERFORMANCE TESTING. The SECON implementation process must be evaluated...
App. A, Section 1, Chap. II, II-4	6.	[Added language]	PROTECTION MEASURES. The SECON response plan should include site-specific protection measures such as...
App. A, Section 1, Chap. II, II-4	7.	[Added language]	...facility...
App. A, Section 1, Chap. II, II-4	8.a.	... DOE O 150.1...	... DOE O 150.1A. ...

Page	Paragraph	Changed	To
App. A, Section 1, Chap. II, II-5		[Added Attachment]	ATTACHMENT 1. SECON Suggested Protection Measures...
App. A, Section 1, Chap. III, III- 1	2	All facilities with assets requiring a facility security clearance . . .	All facilities/sites (as defined in paragraphs 3.a. and b., Section 1 of this Appendix) with assets requiring a facility security clearance. . .
App. A, Section 2, 2-2	4.e	(Note: ISLs do not automatically impose requirements, but may contain useful clarifications. . .)	(Note: ISLs do not automatically impose requirements on DOE, but may contain useful clarifications...) [Writer's Note: this change has been made wherever the ISLs are included in reference lists.]
App. B, Section 1, 1-2	4.k	Directive-Type Memoranda (DTM) issued by the Office of the Under Secretary of Defense (e.g., DTM 09-019, "Policy Guidance for Foreign Ownership, Control, or Influence), available at. . . Note: DTMs, which may be issued periodically. . . do not automatically impose requirements. . .	Directive-Type Memoranda (DTM) issued by the Office of the Under Secretary of Defense, available at. . . Note: DTMs, which may be issued periodically. . . do not automatically impose requirements on DOE. . . [Writer's Note: this change has been made wherever the DTM are included in reference lists.]
App. B, Section 1, 1-2	4.n	DOE O 475.2A, <i>Identifying Classified Information</i> , dated 2- 1-11	DOE O 475.2B, <i>Identifying Classified Information</i> , dated 10-3-14

Page	Paragraph	Changed	To
App. B, Section 1, Chap. I, 1-2	1.c	KMP must be in process for or possess active security clearances in order for a contractor to be eligible for an FCL involving classified information or matter, or SNM.	KMP must possess final active security clearances in order for a contractor to be eligible for a final FCL involving classified information or matter, or SNM. Interim security clearances may be granted to KMP once their background investigations are in process and appropriate additional checks as required in DOE O 472.2, <i>Personnel Security</i> , change 1, have been conducted.
App. B, Section 1, Chap. III, III- 1	2.h	Access authorizations for KMP who . . . must possess or be in the process of obtaining access authorizations equivalent to the level of the facility clearance. (NOTE: until the required KMP access authorizations are finalized, only an interim FCL can be granted.	Access authorizations for KMP who . . . must possess or be in the process of obtaining final access authorizations equivalent to the level of the facility clearance. (NOTE: until the required KMP access authorizations are finalized, only an interim FCL can be granted. In support of an interim FCL, KMP who do not possess clearances must be granted interim access authorizations.)
App. B, Section 1, Chap. IV, IV- 1	1.a	When final access authorizations have been granted to all facility employees, a final FCL must be granted. . .	When final access authorizations have been granted to all facility personnel required to be cleared in connection with the FCL, a final FCL must be granted. . .

Page	Paragraph	Changed	To
App. B, Section 1, Chap. VII, VII-2	3	REGISTERING WORK FOR OTHERS ACTIVITIES. The requirements of DOE O 481.1C, <i>Work for Others (Non-Department of Energy Funded Work)</i> , dated 1-24-05 must be met before a WFO project or any “out of scope” modifications to existing WFO agreements are accepted. WFO activities must be registered in SSIMS.	REGISTERING STRATEGIC PARTNERSHIP PROJECTS (SPP) ACTIVITIES. The requirements of DOE O 481.1C, administrative change 2, <i>Strategic Partnership Projects [Formerly Known as Work for others (Non-Department of Energy Funded Work)]</i> , dated 1-24-05 must be met before an SPP project or any “out of scope modifications to existing SPP agreements are accepted. SPP activities must be registered in SSIMS. [Writer’s Note: “WFO” has been replaced with “SPP” wherever it appears in the document.]
App. B, Section 1, Chap. VII, VII-4	4.b	. . . however, each accredited SCI facility (SCIF) must be registered in SSIMS. however, each accredited SCI facility (SCIF) must be recorded in SSIMS. . .
App. B, Section 2, 2-2	4.f	Directive-Type Memorandum 09-019 (DTM) “Policy Guidance for Foreign Ownership, Control, or Influence,” issued by the Office of the Under Secretary of Defense. . .	Directive-Type Memoranda issued by the Office of the Under Secretary of Defense. . .
App. B, Section 3, 3-1	4.h	DOE O 475.2A, <i>Identifying Classified Information</i> , dated 2-1-11	DOE O 475.2B, <i>Identifying Classified Information</i> , dated 10-3-14
App. B, Section 3, 3-4	4.b.(1)(a) <u>5</u>	. . . contained in DOE O 475.2A	. . . contained in DOE O 475.2B

Page	Paragraph	Changed	To
App. B, Section 4, 4-3	5.g	...a senior Federal official at the site verifies through DOE.a senior Federal official at the site authorized to act as the ODFSA for this purpose verifies through DOE. . .
App. B, Section 4, 4-4	6.d	...approval by DOE/NNSA Federal officials authorized.approval by DOE/NNSA ODFSA authorized. . .
App. B, Section 5, 5-1	4.c	DOE O 350.1, chg. 3	DOE O 350.1, chg. 5
App. B, Section 5, 5-1	4.f	DOE O 414.1D	DOE O 414.1D, admin. change 1
Att. 1, 3	4.b	[Added definition and adjusted following sub-paragraphs accordingly]	Officially Designated Federal Security Authority (ODFSA) means a Federal employee who possesses the appropriate knowledge and responsibilities for each activity to which they are assigned through written delegation of authority.
Att. 1, 3	4.c	[Added definition and adjusted following sub-paragraph accordingly]	Officially Designated Security Authority (ODSA) means a Federal or contractor employee who possesses the appropriate knowledge and responsibilities for each activity to which they are assigned through written delegation of authority.
Att. 1, 3	4.d	...https://pir.labworks.org	...https://pir.doe.gov
Att. 2, Section 1, 1-2	4.e	... , <i>Physical Security Criteria for Federal Facilities</i>	... , August 2013/1 st Edition, <i>Risk Management Process</i>
Att. 2, Section 1, 1-2	4.f.	ISC Standard, <i>Facility Security Level Determination for Federal Facilities</i> .	Cancelled reference removed and subsequent sub-paragraphs re-lettered.
Att. 2, Section 1, 1-2	4.g	ISC Report, <i>The Design Basis Threat (DBT)</i>	ISC Guide, <i>Design Basis Threat</i> , September 2014/9 th Edition

Page	Paragraph	Changed	To
Att. 2, Section 1, 1-2	4.j	HSPD 3, <i>Homeland Security Advisory System</i>	PPD-7, <i>National Terrorism Advisory System</i>
Att. 2, Section 1, 1-2	4.k.	DOE O 151.1, <i>Continuity Programs</i> , dated 5-8-08	DOE O 151.1A, <i>Continuity Programs</i> , dated 3-31-14
Att. 2, Section 1, 1-2	4.l.	[Added reference]	PPD-21, <i>Critical Infrastructure Security and Resilience</i>
Att. 2, Section 1, Chap. II, II-2	3	Each facility or site must identify the specific measures that will most efficiently and effectively implement the required increases in readiness at each SECON level.	Each facility or site must identify the specific measures that will most efficiently and effectively implement the required increases in readiness at each SECON level for that location.
Att. 2, Section 1, Chap. II, II-2	3	Protection measures listed in HSPD-3 and the DOE SECON Quick Reference tool (http://www.hss.energy.gov/Referencebook/secon.html) may be used to develop response plans which must describe the specific actions to be taken for each SECON level.	Response plans must describe the specific actions to be taken for each SECON level.
Att. 2, Section 1, Chap. II, II-2	4.a	...in consultation with the Under Secretaries, the Director, Office of Intelligence and Counterintelligence, and the Chief Health, Safety and Security Officer.	...in consultation with the Under Secretaries; the Director, Office of Intelligence and Counterintelligence; Deputy Under Secretary for Counterterrorism and Counterproliferation, the Associate Under Secretary for Environment, Health, Safety and Security; and the Chief Security Officers for NNSA, Science and Energy, and Management and Performance.
Att. 2, Section 1, Chap. II, II-2	4.a	...DOE O 150.1...	...DOE O 150.1A...

Page	Paragraph	Changed	To
Att. 2, Section 1, Chap. II, II-2	4.a	. . .may require concurrent changes in the SECON level.	. . .may require concurrent changes in the SECON level. If a determination is made by the responsible DOE officials to change the Departmental SECON level, the information will be disseminated through the Emergency Operations Center and any other means deemed appropriate by the Deputy Secretary.
Att. 2, Section 1, Chap. II, II-2	4.b	Local SECON levels may differ from the Departmental SECON level and may be established by the DOE cognizant security office in consultation with contractor site/facility management. The DOE cognizant security office must obtain the concurrence of the cognizant Under Secretary or, in the case of DOE Headquarters, the Chief Health, Safety and Security Officer.	Local SECON levels may differ from the Departmental SECON level in response to local conditions, and may be established by the DOE cognizant security office in consultation with contractor site/facility management. The DOE cognizant security office must obtain the concurrence of the cognizant Under Secretary and the cognizant Chief Security Officer, or, in the case of DOE Headquarters, the Associate Under Secretary for Environment, Health, Safety and Security.
Att. 2, Section 1, Chap. III, III-1	2	All facilities with assets requiring a facility security clearance . . .	All facilities/sites (as defined in paragraphs 3.a. and b., Section 1 of this Attachment) with assets requiring a facility security clearance. . .
Att. 3, Section 1, 1-2	4.k	Directive-Type Memorandum (DTM) 09-019 issued by the Office of the Under Secretary of Defense. . .	Directive-Type Memoranda issued by the Office of the Under Secretary of Defense. . .
Att. 3, Section 1, 1-2	4.n	DOE O 475.2A, <i>Identifying Classified Information</i> , dated 2-1-11	DOE O 475.2B, <i>Identifying Classified Information</i> , dated 10-3-14

Page	Paragraph	Changed	To
Att. 3, Section 1, Chap. I, -1	1.c	KMP must be in process for or possess active security clearances in order for a contractor to be eligible for an FCL involving classified information or matter, or special nuclear material (SNM).	KMP must possess final active security clearances in order for a contractor to be eligible for a final FCL involving classified information or matter, or special nuclear material (SNM). Interim security clearances may be granted to KMP once their background investigations are in process and appropriate additional checks as required in DOE O 472.2, <i>Personnel Security</i> , change 1, have been conducted.
Att. 3, Section 1, Chap. III, III- 1	2.h.	Access authorizations for key management personnel (KMP) who . . . must possess or be in the process of obtaining access authorizations equivalent to the level of the facility clearance. (NOTE: until the required KMP access authorizations are finalized, only an interim FCL can be granted.	Access authorizations for key management personnel (KMP) who . . . must possess or be in the process of obtaining final access authorizations equivalent to the level of the facility clearance. (NOTE: until the required KMP access authorizations are finalized, only an interim FCL can be granted. In support of an interim FCL, KMP who do not possess clearances must be granted interim access authorizations.)
Att. 3, Section 2, 2-2	4.f	. . .(e.g., DTM 09-019, “Policy Guidance for Foreign Ownership, Control, or Influence” issued 9-2-09),.available at http://www.dtic.mil/whs/directives/corres/dir3.html . (Note: DTMs, which may be issued periodically on a variety of topics, do not automatically impose requirements on DOE, but may contain useful information applicable to existing NISP programs.)
Att. 3, Section 3, 3-1	4.h	DOE O 475.2A, <i>Identifying Classified Information</i> , dated 2-1-2011	DOE O 475.2B, <i>Identifying Classified Information</i> , dated 10-3-14

Page	Paragraph	Changed	To
Att. 3, Section 3, 3-4	6.b.(1)(a) <u>5</u>	. . . contained in DOE O 475.2A	. . .contained in DOE O 475.2B
Att. 3, Section 4, 4-3	5.g	. . .has been approved for such access by the facility/site's authorized DOE Federal official,has been approved for such access by the facility/site's authorized ODFSA for this purpose, . . .
Att. 3, Section 4, 4-4	6.d	. . .approval by DOE/NNSA Federal officials authorized.approval by DOE/NNSA ODFSA authorized. . .
Att. 3, Section 5, 5-1	4.b	DOE O 350.1 chg. 3	DOE O 350.1 chg. 5
Att. 3, Section 5, 5-1	4.d	DOE O 414.1D	DOE O 414.1D, admin. change 1
Att. 5, 5	4.v	DOE O 232.2	DOE O 232.2, administrative change 1
Att. 5, 5	4.w	. . . <i>Security Incident (Including Cyber) Notification Protocol</i> , dated 6-2-11. <i>Security Incident (Including Cybersecurity) Notification Protocol</i> , dated 8-23-13. . .
Att. 5, 7	5.c(3)	. . .DOE O 475.2A, <i>Identifying Classified Information</i> , dated 2-1-11.DOE O 475.2B, <i>Identifying Classified Information</i> , dated 10-3-14. . .
Att. 5, Section 1, 1-2	2.c.(2)	. . .; therefore, MI incidents do not require formal inquiry, closure, etc.	. . .; therefore, MI incidents do not require formal inquiry, closure, etc., but must still be categorized as A or B.
Att. 5, Section 1, 1-6	3.f.(1)	Per DOE O 232.2, <i>Occurrence Reporting and Processing of Operations Information</i> . . .	Per DOE O 232.2, <i>Occurrence Reporting and Processing of Operations Information</i> , admin. chg. 1,. . .
Att. 5, Section 1, 1-7	3.f.(7)	Per DOE M 205.1-8 Admin Chg 2, <i>Cyber Security Incident Management Manual</i> , dated 1-08-09. . .	Per DOE O 205.1B, Chg 3, <i>Department of Energy Cyber Security Program</i> , dated 5-16-11. . .