U.S. Department of Energy
Washington, DC

LIMITED CHANGE

DOE O 205.1C

Chg 1 (LtdChg): 2-3-2022

SUBJECT: LIMITED CHANGE TO DOE O 205.1C, *DEPARTMENT OF ENERGY CYBERSECURITY PROGRAM*

1. EXPLANATION OF CHANGES. This Limited Change adds the Department's Vulnerability Disclosure Program .

2. LOCATIONS OF CHANGES:

Page	Paragraph	Changed	To
1	3.b.	Department of Energy (DOE) Contractors. Except for the equivalencies/ exemptions in paragraph 3.c., the CRD, Attachment 1, sets forth requirements of this Order that will apply to certain Management and Operating (M&O) contracts and non-M&O Major Site/Facility contracts as determined by the Heads of Departmental Elements (HDEs).	Department of Energy (DOE) Contractors. Except for the equivalencies/ exemptions in paragraph 3.c., the CRD, Attachment 1, sets forth requirements of this Order, including those requirements contained in Attachment 2, that will apply to certain Management and Operating (M&O) contracts and non-M&O Major Site/Facility contracts as determined by the Heads of Departmental Elements (HDEs).
4	4.c.(4)	For Controlled Unclassified Information (CUI), Official Use Only (OUO), and Unclassified Controlled Technical Information (UCTI) on Non-Federal systems, DEs/Sites must adhere to the security requirements specified in NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. Information that may be categorized as "CUI Specified" in accordance with the requirement of 32 CFR 2002 may have additional protection requirements specified by the applicable CUI-specified owner.	For Controlled Unclassified Information (CUI), Official Use Only (OUO), and Unclassified Controlled Technical Information (UCTI) on Non-Federal systems, DEs/Sites must adhere to the security requirements specified in NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. Information that may be categorized as "CUI Specified" in accordance with the requirement of 32 CFR 2002 may have additional protection requirements specified under law, regulation, or Government-wide policies (LRGWP). Where the LRGWP does not address security requirements, the

Page	Paragraph	Changed	To
			security requirements specified in NIST SP 800-171 apply.
5	4.e.	Common CSPP Topics. The E-CSPP and DE/Site-CSPPs must address requirements for the following items in accordance with the Federal laws, regulation, directives, policies, standards, and guides pertaining to cybersecurity, as well as interrelated DOE issuances, directives, policies, and procedures identified in Attachment 2:	Common CSPP Topics. The E-CSPP and DE/Site-CSPPs must address requirements for the following items in accordance with the Federal laws, regulation, directives, policies, standards, and guides pertaining to cybersecurity, as well as interrelated DOE issuances, directives, policies, and procedures identified in Attachment 3:
7	4.f.(4)(c)	Added.	iJC3 operations must comply with review requirements for documents that potentially contain classified information or Unclassified Controlled Nuclear Information (UCNI) under DOE O 475.2, *Identifying Classified information*, current version; and Title 10 Code of Federal Regulations (CFR), Part 1017, *Identification and Protection of Unclassified Controlled Nuclear Information.*
7	4.f.(4)(c)-(d)	Renumbered.	4.f.(4)(d)-(e)
8	4.f.(8)	Added.	Vulnerability Disclosure Program. Attachment 2 sets forth requirements and handling procedures for the Department's Vulnerability Disclosure Program in alignment with the Office of Management and Budget (OMB) Memorandum (M)-20-32, *Improving Vulnerability Identification, Management, and Remediation* and the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directive (BOD) 20-01, *Develop and Publish a Vulnerability Disclosure Policy*. (a) Implement a Vulnerability Disclosure Program (VDP) in

Page	Paragraph	Changed	To
			alignment with OMB M-20-32, *Improving Vulnerability Identification, Management, and Remediation* and BOD 20-01, *Develop and Publish a Vulnerability Disclosure Policy*, and formalize a mechanism to receive information from external third parties about potential security vulnerabilities on public facing and internet-accessible DOE systems and websites. (b) Establish triage and assessment processes for reported vulnerabilities by external third parties. (c) Maintain communication with external third parties on reported vulnerabilities. (d) Track reported vulnerabilities in alignment with risk management and incident reporting metrics and processes.
9	4.f.(8)-(10)	Renumbered.	4.f.(9)-(11)
9	4.h.	Coordination and any deviations involving COMSEC requirements must come from the DOE COMSEC COR to the appropriate National Authority.	Coordination for deviations involving COMSEC requirements must come from the DOE COMSEC COR to the appropriate National Authority.
11	4.i.(6)(b)	Must include requirements for protecting Restricted Data (RD), Formerly Restricted Data (FRD) and Transclassified Foreign Nuclear Information (TFNI) on NSS consistent with DOE O 471.6, *Information Security*, current version, and DOE O 452.8, *Control of Nuclear Weapon Data*, current version. When RD, FRD, or TFNI is provided to personnel from other Government Agencies, the CSPPs must ensure that such personnel follow the	Must include requirements for identifying and protecting Restricted Data (RD), Formerly Restricted Data (FRD) and Trans-classified Foreign Nuclear Information (TFNI) on NSS consistent with DOE O 471.6, *Information Security*, current version; DOE O 475.2, *Identifying Classified Information*, current version; and DOE O 452.8, *Control of Nuclear Weapon Data*, current version. When RD, FRD, or TFNI is provided to personnel

Page	Paragraph	Changed	To
		requirements contained in this Order.	from other Government Agencies, the CSPPs must ensure that such personnel follow the requirements contained in this Order.
12	4.i.(8)(b)	Added.	A definition of information system that includes the computer, the DOE computer network, and all devices, such as storage media, connected to the computer;
12	4.i.(8)(b)-(d)	Renumbered.	4.i.(8)(c)-(e)
12	4.i.(8)(g)	Renumbered.	Was 4.i.(8)(e)
16	5.c.(9)	Added.	Participate in and support execution of the Vulnerability Disclosure Program with overall responsibility for the remediation of vulnerabilities reported on systems and services deemed to be in-scope for the program.
16-17	5.c.(9)-(12)	Renumbered.	5.c.(10)-(13)
19	5.d.(7)	Serves as, designates or delegates other required Senior Accountable Official roles related to cybersecurity as approved by S2.	Serves as the designee or delegates other required Senior Accountable Official roles related to cybersecurity as approved by S2.
22	5.n.	… See charters referenced in Attachment 2.	… See charters referenced in Attachment 3.
23	6.	Added.	INVOKED STANDARDS. This Order does not invoke any DOE technical standards or industry standards as required methods. Any technical standard or industry standard that is mentioned in or referenced by this Order is not invoked by this Order. Note: DOE O 251.1D, Appendix J provides a definition for "invoked technical standard."
23	6.-9.	Renumbered.	7.-9.
23	7.	REFERENCES. Attachment 2 provides published laws, rules, regulations, policy, directives, standards, guidance and other issuances cited and additional	REFERENCES. Attachment 3 provides published laws, rules, regulations, policy, directives, standards, guidance and other issuances cited and additional

Page	Paragraph	Changed	To
		information sources to assist in implementing this Order.	information sources to assist in implementing this Order.
23	8.	DEFINITIONS AND ACRONYMS. Attachment 3 provides definitions and acronyms.	DEFINITIONS AND ACRONYMS. Attachment 4 provides definitions and acronyms.
Attachment 1, Contractor Requirements Document			
1-1	Second Paragraph	Added.	In addition to the requirements set forth in this CRD, contractors are responsible for complying with Attachment 2 to DOE O 205.1C, referenced in and made a part of this CRD, which provides information and requirements applicable to contracts in which this CRD is inserted.
1-1	1.g.	Added.	Establish and maintain a process to support the Vulnerability Disclosure Program for vulnerabilities reported to in-scope DOE websites and systems.
1-1	1.g.-h.	Renumbered.	1.h.-i.
1-2	2.e.	Implement requirements for accessing and protecting Restricted Data (RD), Formerly Restricted Data (FRD) and Transclassified Foreign Nuclear Information (TFNI) as defined in the DE-CSPPs.	Implement requirements for accessing, identifying and protecting Restricted Data (RD), Formerly Restricted Data (FRD) and Trans-classified Foreign Nuclear Information (TFNI) as defined in the DE-CSPPs.
Attachment 2, Vulnerability Disclosure Program (VDP) Policy and Handling Procedures			
2-1 – 2-10		Added.	This is an entirely new attachment.
Attachment 3, References			
3-1	1.e.	Added.	Title 32 Code of Federal Regulations (CFR) § 2002, Controlled Unclassified Information (CUI).
3-1	1.e.-g.	Renumbered.	1.f.-h.
3-2	5.	DOE ORDERS, MANUALS, NOTICES, AND GUIDELINES.	DOE ORDERS AND GUIDELINES.

Page	Paragraph	Changed	To
3-3	5.p.	DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*.	Removed.
3-3	5.q.-t.	Renumbered.	5.p.-s.
3-3	5.u.	DOE P 205.1, *Departmental Cyber Security Management Policy*.	Removed.
Attachment 4, Definitions and Acronyms			
4-3	Acronyms Table	Added.	IP – Intellectual Property
4-3	Acronyms Table	Management and Operations	Management and Operating
4-3	Acronyms Table	Management and Operations	Management and Operating
4-3	Acronyms Table	Transclassified Foreign Nuclear Information	Trans-classified Foreign Nuclear Information
4-3	Acronyms Table	Added.	VDP – Vulnerability Disclosure Program