Response to Public Comments on Draft Regulatory Guide (DG)-5044
"Insider Mitigation Program"
Proposed Revision 1 of Regulatory Guide (RG) 5.77

On January 4, 2016, the NRC released Draft Regulatory Guide, DG-5044 (Proposed Revision 1 of RG 5.77) for a 60-day comment period to external stakeholders with a need-to-know. Since DG-5044 was Official Use Only – Security Related Information, the NRC did not make the document publicly available or publish a Federal Register Notice to open a public comment period. To facilitate stakeholder comment, the NRC staff provided DG-5044 to the Nuclear Energy Institute (NEI) for distribution to authorized industry stakeholders. In addition, Dr. Edwin Lyman of the Union of Concerned Scientists (UCS) visited the NRC headquarters office to review a copy of DG-5044 and to provide comments. Dr. Lyman has a clearance and provides perspectives on the security issues set forth in DG-5044 as an informed member of the public. The comment period ended on February 29, 2016. The NRC received 81 comments from NEI and 4 comments from UCS. On October 7, 2016, the NRC received 11 more comments from NEI and 4 more comments from UCS. The NRC has combined all comments and the NRC staff responses in the following table.

Comments were received from the following:

David R. Kline
Director, Security
Nuclear Energy Institute (NEI)
1201 F Street, NW Suite 1100
Washington, DC 20004
(ADAMS Accession Nos. ML16281A605 and ML16062A349)

Edwin Lyman,
Union of Concerned Scientists (UCS)
ELyman@ucsusa.org
(Comments were provided at meetings with NRC staff)

For each comment received, the "Specific Comments" column presents the DG-5044 language referenced by the commenter, if applicable, along with the commenter's verbatim comment statement and any suggested revisions proposed by the commenter.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
1. NEI	A. Introduction, Applicable Rules and Regulations (Page 2)	DG-5044 language: …Furthermore, 10 CFR 73.55(b)(9)(i) states that the IMP must monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization to a protected or vital area, and implement defense-in-depth methodologies to minimize the potential for an insider to adversely	The NRC disagrees with the comment. It appears there may be confusion about the requirements of unescorted access authorization (UAA) and unescorted access (UA). UAA is the act of certifying by the licensee's reviewing official that the applicant's background investigative elements within the authorization process have been satisfactorily completed and all the required

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		affect, either directly or indirectly, the licensee's capability to prevent significant core damage and spent fuel sabotage. NEI comment: The term "unescorted access authorization" (UAA) should be "unescorted access" as UAA represent the clearance for UA. The word "retaining" should be "maintaining." The change represents consistency with the industry understanding of the use of the terms. The commenter proposed the following edits: "…Furthermore, 10 CFR 73.55(b)(9)(i) states that the IMP must monitor the initial and continuing trustworthiness and reliability of individuals granted or ~~retaining~~ maintaining unescorted access ~~authorization~~ to a protected…".	elements for granting unescorted access is certified prior to granting access to the protected area. The UAA determination is evaluated by a licensee reviewing official who then makes a favorable determination relative to the individual's trustworthiness, reliability, and fitness-for-duty. UA is granted to an individual only after satisfactorily completing all the regulatory requirements for UAA and the individual has completed plant access training; is subjected to a behavioral observation program; is placed in a random drug and alcohol testing program; and is provided the physical means to gain UA to the protected area. Accordingly, the NRC has made no change to DG-5044 based on this comment.
2. NEI	A. Introduction, Applicable Rules and Regulations (Page 2)	DG-5044 language: 10 CFR Part 26, "Fitness for Duty Programs," (Ref. 4), in part states, that fitness for duty programs must provide reasonable assurance that individuals are trustworthy and reliable as demonstrated by the avoidance of substance abuse; individuals are not under the influence of any substance, legal or illegal, or mentally or physically impaired from any cause, which in any way adversely affects their ability to safely and competently perform their duties; and the workplaces subject to Part 26 are free from the presence and effects of illegal drugs and alcohol, and provide reasonable measures for the early detection of individuals who are not fit to perform	The NRC disagrees with the comment. The language contained in this paragraph has been taken from the regulation found under 10 CFR 26.23 (a)-(e) performance objectives and is appropriately applied in this paragraph. Therefore, the language suggested by the commentator is not necessary. Accordingly, the NRC has made no change to DG-5044 based on this comment.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		the duties that require them to be subject to the Fitness for Duty (FFD) program. NEI comment: In the text the term “illegal drugs” is only one objective component of Part 26. The paragraph should be expanded to include “the use of illegal drugs, the abuse of prescribed or over the counter medications, or the excessive, habitual use of alcohol. The commenter proposed the following edits: “...subject to Part 26 are free from ~~the presence and effects of illegal drugs and alcohol~~, the use of illegal drugs, the abuse of prescribed or over the counter medications, or the excessive, habitual use of alcohol and provide reasonable measures for...”	
3. NEI	A. Introduction, Applicable Rules and Regulations (Page 2)	DG-5044 language: 10 CFR 50.82, “Termination of license,” paragraph (a)(1)(i), requires that when a licensee has determined to permanently cease operations the licensee shall, within 30 days, submit a written certification to the NRC, consistent with the requirements of § 50.4(b)(8). NEI comment: The industry believes that decommissioning should be discussed ins [sic] a separate decommissioning document. Delete	The NRC agrees with the comment to delete the reference to 10 CFR 50.82, “Termination of license.” However, the NRC disagrees that DG-5044 should not include guidance on insider mitigation programs during decommissioning. The NRC did publish in the *Federal Register* on March 3, 2022, a proposed rule titled, “Regulatory Improvements for Production and Utilization Facilities Transitioning to Decommissioning” (87 FR 12254). The proposed rule is seeking to amend NRC regulations principally related to the decommissioning of nuclear power reactors. As part of this proposed rule, the staff proposes changes to correct inconsistencies in the

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
			10 CFR Part 26 Fitness for Duty (FFD) program requirements and to clarify FFD program provisions pertaining to a licensee's insider mitigation program under 10 CFR 73.55(b)(9). The March 7, 2018, SECY-18-0055 described the relationship of this decommissioning rulemaking to several guidance documents, one of which was RG 5.77 (ADAMS Accession No. ML18012A021). Enclosure 3 to SECY-18-0055 stated that "The NRC staff will ensure that RG 5.77 is revised if necessary to be consistent with the final rule." (ML18012A228)
4. NEI	A. Introduction, Related Guidance, 2nd Bullet (Page 2)	DG-5044 language: Regulatory Guide (RG) 5.69, "Guidance for the Application of the Radiological Sabotage Design-Basis Threat in the Design, Development, and Implementation of a Physical Security Program that meets 10 CFR 73.55 Requirements," (SGI) (Ref. 6), provides a description of and guidance for mitigating the active insider, and passive insider. NEI comment: For consistency between documents ensure that that active insider and passive insider are consistent with Regulatory Guide 5.62.	The NRC agrees with this comment and has confirmed that the treatment of an active or passive insider in DG-5044 (RG 5.77) is consistent with the treatment of an active or passive insider in RG 5.69. The NRC believes that the commenter inadvertently referred to RG 5.62, "Reporting of Physical Security Events," instead of RG 5.69, which addresses an active and passive insider. Accordingly, the NRC has made no change to DG-5044 based on this comment.
5. NEI	B. Discussion, Reason for Revision, 2nd Paragraph (Page 5)	DG-5044 language: In addition, this revision provides licensees with guidance for continuing to meet requirements for an IMP following the licensee's determination to permanently cease operations and permanent removal of fuel from the reactor vessel in	The NRC disagrees with the comment to remove the reference to 10 CFR 50.82(a)(1)(i)-(ii). However, the NRC has revised DG-5044 to state: "In addition, this revision provides licensees with guidance for continuing to meet the requirements

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		accordance with 10 CFR 50.82(a)(1)(i) and 10 CFR 50.82(a)(1)(ii), respectively. NEI comment: The industry suggests removal of this section and to include the section within a separate decommissioning rule-making.	for an IMP following the licensee's determination to permanently cease operations and remove fuel from the reactor vessel in accordance with 10 CFR 50.82(a)(1)." The NRC response to Comment Number 3 also applies to this comment.
6. NEI	C.1. General Requirements, 1st Paragraph, Last sentence, (Page 7)	DG-5044 language: (OUO-SRI) … Licensees should consider and be observant of subtle changes in an individual's behavior or actions over time and use appropriate IMP elements (e.g., the behavioral observation program) to assess and mitigate potential adverse acts by insiders. NEI comment: In this section the licensee's BOP is required to also take action due to an individual's behavior that can change quickly so the last sentence should be improved upon to address both, not just behavior that can happen overtime. The last sentence is in need of a period at the end of the sentence. The commenter proposed the following edits: "…Licensees should consider and be aware of typical conditions which trigger behavioral anomalies such as being observant of subtle changes in an individual's behavior or actions over time or recognition that changes in emotional state can happen quickly and use appropriate IMP elements (e.g., the behavioral observation program) …"	The NRC agrees with the intent of the comment but has not accepted the specific revisions suggested by the commenter. Instead, the NRC has revised DG-5044 to state: "Licensees should consider and be observant of subtle changes in an individual's behavior or actions over time and use appropriate IMP elements (e.g., the behavioral observation program) to assess not only the individual's trustworthiness and reliability but to gain insights into his or her character and reputation (10 CFR 73.56(d)(6)) to aid in the licensee reviewing official's access authorization assessment and perhaps prevent the individual from executing subversive acts." The revision provides alignment under the character and reputation requirements of 10 CFR 73.56(d)(6) to include the typical conditions that may trigger behavioral anomalies that are required to be reported under behavioral observation. This section in DG-5044 provides a high-level discussion of the general requirements for an

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
			insider mitigation program. Specific attributes of behavior observation characteristics are provided in Section 4, Behavior Observation Training, of DG-5044. The "Official Use Only—Security Related Information" (OUO-SRI) portion marking in this section, as well as the markings appearing throughout DG-5044 have been removed by the NRC staff in the Office of Nuclear Security and Incident Response consistent with the Commission direction in the Staff Requirements Memorandum (SRM)—SECY-17-0095—Review and Approval of Proposed Revision to RG 5.77, "Insider Mitigation Program," dated July 14, 2021 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML21195A356). The staff critically examined the designation of all information in DG-5044 and determined that it should not be designated as OUO-SRI. DG-5044 will now be available for public release.
7. NEI	C.1. General Requirements, 2nd Paragraph, 2nd Sentence (Page 7)	DG-5044 language: …As set forth in 10 CFR 73.55(b)(9)(i), nuclear power reactor licensees are required to establish, maintain, and implement an IMP to monitor the initial and continuing trustworthiness and reliability of individuals granted unescorted access or unescorted access authorization, or retaining unescorted access or unescorted access authorization to a protected or vital area. The IMP must implement defense-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, a	The NRC disagrees with the comment. 10 CFR 73.55(b)(9)(i) states in part, "The insider mitigation program must monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization to a protected or vital area…". Therefore, the language in DG-5044 more closely aligns with the regulation under 10 CFR 73.55(b)(9)(i) than does the comment's proposed revision. Furthermore, the requirements found under 10 CFR 73.55(b)(9)(i) take into consideration the requirements for the granting of unescorted

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		licensee's capability to prevent significant core damage or spent fuel sabotage. NEI comment: The text discusses "individuals granted unescorted access or unescorted access authorization, or retaining unescorted access or unescorted access authorization to a protected or vital area." Consideration should be given to a more consistent use of the terms unescorted access authorization and unescorted access and maintaining (retaining) of each. The suggested change text if [sic] provided for consideration. The commenter also proposed the following edits: "…an IMP to monitor the initial and continuing trustworthiness and reliability of individuals ~~granted unescorted access or unescorted access authorization, or retaining unescorted access~~ granted unescorted access or maintaining unescorted access authorization to a…"	access or maintaining unescorted access authorization as part of the performance requirement to monitor the continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization. Accordingly, the NRC has made no change to DG-5044 based on this comment.
8. NEI	C.1 General Requirements, 3rd Paragraph (Page 7)	NEI comment: This paragraph describes that an important focus for an IMP program is the implementation of measures that control personnel access to digital computer, communication systems, and computer networks. Concern: The scope of digital computer and communications systems and networks included within the scope of the cyber security rule exceeds the set of systems and equipment within a nuclear	The NRC disagrees with the comment. The insider mitigation program (IMP) is required by 10 CFR 73.55(9). Consistent with 10 CFR 73.55(b)(9)(i), the IMP must monitor the initial and continuing trustworthiness and reliability of individuals granted unescorted access and unescorted access authorization. As stated, the foundation of the insider mitigation program is to ensure that licensees "implement defense-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee's capability to prevent

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		power plant that, if subject to action by an internal threat, would be inimical to the common defense and security, or the public health and safety. For example, there are CDAs (e.g., EP EOF, certain security telecommunications) that IT supports who do not have unescorted access and are not under the standard IMP for Nuclear Badged employees. Additionally, in 2010, the scope of the term "important to safety" as used in the cyber security rule was expanded to include SSCs in the balance-of-plant that were not within the scope of the cyber rule when it was promulgated. The protection measures of Cyber Security Plans are implemented to provide high assurance that CDAs outside the protected area will not pose a threat to the safety and security of the plant (Refer to 1.1 pg. 8) Recommendation: The RG should provide, as discussed more fully elsewhere in these comments, a graded approach to the implementation of the IMP. The suggested wording provides flexibility to support a graded approach. The commenter proposed the following edits: "…vital areas, and accessible target set locations in addition to digital computer, communication systems, and computer networks that, if compromised by a cyber attack, would be inimical to the common defense and security, or the public health and safety. ~~associated with: safety related and important to safety functions; security~~	significant core damage and spent fuel sabotage." Consistent with 10 CFR 73.55(b)(9)(ii), the IMP must contain elements from the cyber security program described in 10 CFR 73.54. The NRC's cyber security rule specifically requires the protection of those digital computer and communication systems associated with safety-related and important to safety-functions, security functions, or emergency preparedness functions, and support systems that if compromised would adversely impact these functions. Therefore, the NRC has determined that it is appropriate to reference these functions in this guidance. Accordingly, the NRC has made no change to DG-5044 based on this comment.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		~~functions; emergency~~ ~~preparedness functions, including off~~ ~~site communications; and, support systems and equipment that, if~~ ~~compromised, would adversely~~ ~~impact safety, security, or emergency preparedness functions.~~"	
9. NEI	C.1 General Requirements, 3rd Paragraph, 1st Sentence (Page 8)	DG-5044 language: Licensees should perform an analysis of their programs and industry or other insider related events to ensure that their policies, actions, and measures provide a level of protection that meets the IMP requirements. NEI comment: The industry needs a trigger point from which it can depend upon reliable information. It would seem that substantiated fact-based events contained within Information Notices (IN), Regulatory information summaries (RIS) or other official accounts of the events. The commenter proposed the following edits: "…Licensees should perform an analysis of their programs and industry or other insider-related events as detailed within NRC Information Notices, Regulatory Information Summaries or other official accounts of the events into ensure that their policies, actions, and measures provide a level of protection that meets the IMP requirements."	The NRC disagrees with the comment. A licensee's assessment and maintenance of its insider mitigation program cannot be limited to NRC Information Notices and Regulatory Information Summaries. Licensees, through access to the daily flow of public information related to terrorist activities, some of which has been perpetrated by an insider, or through information obtained by a licensee or information shared within the industry, may be presented with opportunities that could rise to the level of consideration for self-assessment and analysis resulting in programmatic improvement in the licensee's insider mitigation program. Accordingly, the NRC has made no change to DG-5044 based on this comment.
10. NEI	C.1 General Requirements,	DG-5044 language: Licensee management, acting as or through a designated reviewing official, may grant, deny, suspend, withhold, revoke, or terminate	The NRC agrees with the intent of the comment but has not accepted the specific revision suggested by the commenter. Instead, the NRC has revised DG-5044 to state:

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
	3rd Paragraph, 2nd Sentence (Page 8)	unescorted access authorization or unescorted access; determine what level of access, if any, an individual will have; and, make all final decisions regarding unescorted access to its facilities in accordance with 10 CFR 73.56, integrated with the performance requirements of 10 CFR 73.57, "Requirements for criminal history records checks of individuals granted unescorted access to a nuclear power facility, a non-power reactor, or access to safeguards information," and the escorted access requirements mandated in 10 CFR 73.55(g)(7). NEI comment: The sentence should be simplified to specify the licensee's reviewing official as required by regulation. The sentence seems to specify that the licensee management grants, denies, suspends, withholds, revokes, or terminates unescorted access authorization or unescorted access. The commenter proposed the following edits: "…The licensee's reviewing official, may grant, deny, suspend, withhold, revoke, or terminate unescorted access authorization or unescorted…"	"The licensee's, or applicant's, reviewing official may grant, deny, suspend, withhold, revoke, or terminate unescorted access or unescorted access authorization; determine what level of access, if any, an individual will have; and make all final decisions on unescorted access to its facilities in accordance with 10 CFR 73.56. These requirements are implemented with those of 10 CFR 73.57, "Requirements for criminal history records checks of individuals granted unescorted access to a nuclear power facility, a non-power reactor, or access to safeguards information," and the escorted access requirements mandated in 10 CFR 73.55(g)(7)."
11. NEI	C.1 General Requirements, 3rd Paragraph, 3rd Sentence (Page 8)	DG-5044 language: Licensees should not allow an individual who demonstrates questionable behavior to retain unescorted access. NEI comment:	The NRC does not agree with the commenter's suggested use of the term "aberrant behavior." The Cambridge Dictionary definition of "aberrant" is: "different from what is typical or usual, especially in an unacceptable way." The word "aberrant" does not take into consideration behaviors that can be associated with acts that rise to the level of unusual or uncommon (e.g., unusual interest in, or

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		The term "questionable behavior" should be change [sic] to aberrant behavior a term already defined in the licensee's programs. The commenter proposed the following edit: "Licensees should not allow an individual who demonstrates aberrant behavior to retain unescorted access."	predisposition toward security activities, or behaviors that would arouse suspicions in a reasonable person). The term "questionable behavior" has a different meaning. It more correctly describes the broader perspective conveyed in the guidance in DG-5044. This would include behavior that may be a potential threat in the nuclear power plant such as personnel under the influence of drugs or alcohol where the NRC has maintained a drug free work environment under 10 CFR Part 26. Such behavior would be questionable but may not meet the definition of aberrant behavior. Accordingly, the NRC has made no change to DG-5044 based on this comment.
12. NEI	C.1 General Requirements, 3rd Paragraph, 4th Sentence (Page 8)	DG-5044 language: This degrades the licensee's ability to prevent adverse acts. NEI comment: The industry recommends a change in the sentence to more clearly define the impact. The commenter proposed the following edits: "This degrades the licensee program's preventative measures to provide high assurance that an individual's behavior does not constitute an unreasonable risk to public health and safety,	The NRC agrees with the intent of the comment but has not accepted the specific revision suggested by the commenter. Instead, the NRC has revised DG-5044 to state: "Licensees should not allow an individual who demonstrates questionable behavior (as discussed in 10 CFR Part 26 and 10 CFR 73.56) to retain unescorted access because doing so degrades the licensee's ability to prevent adverse acts." The "high assurance"[1] standard is addressed in DG-5044 in response to Comment Number 15.

[1] In Staff Requirements Memorandum (SRM) SRM-SECY-16-0073, Options and Recommendations for the Force-on-Force Inspection Program in Response to SRM-SECY-14-0088, the Commission stated that "the concept of 'high assurance' of adequate protection found in our security

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		including the potential to commit radiological sabotage."	
13. NEI	C.1 General Requirements, 4th Paragraph (Pages 7-8)	DG-5044 language: As described in 10 CFR 73.56(a), a licensee is required to establish, implement, and maintain an AA program, as a part of its physical security plan, for granting unescorted access to protected and vital areas of a nuclear power plant. This program's objective is to provide high assurance that individuals granted unescorted access are trustworthy and reliable and do not constitute an unreasonable risk to public health and safety, including the potential to commit radiological sabotage. NEI comment: This is a repeat statement and not required. Delete.	The NRC disagrees with this comment. The location of the sentence ensures that licensees and applicants are provided with guidance on the source requirements for the insider mitigation program. Accordingly, the NRC has made no change to DG-5044 based on this comment.
14. NEI	C.1 General Requirements, 2nd Paragraph (Page 8)	DG-5044 language: As described in 10 CFR 73.56(f), "Behavioral observation," 10 CFR 73.56(g), "Self-reporting legal actions," 10 CFR 73.56(i), "Maintaining unescorted access or unescorted access authorization," and 10 CFR 73.56(j), "Access to vital areas," in conjunction with IMP program requirements, licensees are required to ensure, following their initial determination of unescorted access or access authorization, continued trustworthiness and reliability of those with unescorted access to a facility, as well as to	The NRC agrees with the comment and has revised DG-5044 accordingly. In addition, the NRC has revised this paragraph to improve readability by removing the section titles associated with each regulatory requirement. The NRC also removed the sentence "Efforts undertaken to ensure the continued trustworthiness and reliability of individuals granted unescorted access also supports the IMP." The paragraph states:

regulations is equivalent to 'reasonable assurance' when it comes to determining what level of regulation is appropriate." (ADAMS Accession No. ML16279A345).

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		maximize opportunities to identify insider activity. Efforts undertaken to ensure the continued trustworthiness and reliability of individuals granted unescorted access also supports the IMP. NEI comment: Delete "or access "authorization."	"As described in 10 CFR 73.56(f), (g), (i), and (j), in conjunction with the IMP requirements, licensees must ensure, following their initial determination of unescorted access, continued trustworthiness and reliability of those individuals with unescorted access to a facility, as well as maximize opportunities to identify insider activity."
15. NEI	C.1.1, 1st sentence (Page 8)	DG-5044 language: (OUO-SRI) Licensees are required to implement the requirements contained in 10 CFR 73.54, in conjunction with 10 CFR 73.55(b)(9) and 10 CFR Part 26, to provide high assurance that a person with access to digital computer and communications systems and networks from outside the protected area will not pose a significant threat to the safety and security of a nuclear power plant. NEI comment: Reference to the licensee Cyber Security Plan as a key document is appropriate. 10 CFR 26 only requires "reasonable" assurance. The commenter proposed the following edits: "(OUO-SRI) Licensees are required to implement the requirements contained in 10 CFR 73.54 within a licensee cyber security plan, in conjunction with 10 CFR 73.55(b)(9) ~~and 10 CFR Part 26~~, to provide high assurance along with 10 CFR 26 that a person with access to digital computer and communications systems and networks from outside the protected area will not	The NRC agrees with the intent of the comment but has not accepted the specific revision suggested by the commenter. Instead, the NRC has revised DG-5044 to state: "Licensees must implement the required elements of their cyber security plans as they address the requirements in 10 CFR 73.54, 10 CFR 73.55(b)(9), and 10 CFR Part 26, to provide high assurance that a person with access to digital computer and communications systems and networks from outside the protected area will not pose a significant threat to the safety and security of a nuclear power plant." Based on administrative renumbering, this revision now appears under Section C.1 as the last paragraph on page 8 of DG-5044. Licensees are required to provide high assurance that a person with access to digital computer and communications systems and networks from outside the protected area will not pose a significant threat to the safety and security of a nuclear power plant. The high assurance requirement found in 10 CFR 73.54 is supported in

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		pose a significant threat to the safety and security of a nuclear power plant."	part, by licensees implementing associated requirements in 10 CFR 73.55(b)(9) and 10 CFR Part 26. In SRM-SECY-16-0073, Options and Recommendations for the Force-on-Force Inspection Program in Response to SRM-SECY-14-0088, the Commission stated that "the concept of 'high assurance' of adequate protection found in our security regulations is equivalent to 'reasonable assurance' when it comes to determining what level of regulation is appropriate" (ADAMS Accession No. ML16279A345). Accordingly, the NRC has added a footnote to the term "high assurance," as it appears in the "Applicable Rules and Regulations" section of DG-5044 for the discussion of 10 CFR 73.54, that reflects the SRM-SECY-14-0088 information. The NRC staff also removed the "(OUO-SRI)" portion marking from this paragraph, consistent with the Commission direction in the Staff Requirements Memorandum (SRM)—SECY-17-0095—Review and Approval of Proposed Revision to RG 5.77, "Insider Mitigation Program," dated July 14, 2021 (ML21195A356).
16. NEI	C.1.1, 4th Paragraph, Last sentence (Page 8)	DG-5044 language: The potential for significant harm demonstrates the need for an IMP that ensures the trustworthiness and reliability of specific individuals working at, for, or supporting nuclear power plant operations. NEI comment:	The NRC agrees with the intent of the comment but has not accepted the specific revision suggested by the commenter. The potential for significant harm from malicious and willful tampering of sensitive safety- and security-related equipment demonstrates the need for an insider mitigation program that ensures the trustworthiness and reliability of specific individuals working at, for,

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		The paragraph relies upon the trustworthiness and reliability of individuals to mitigate "acts of wrongdoing or overt acts of tampering are particularly serious matters because of the potential adverse impact to the safety and security of the nuclear power plant that could adversely affect the protection of the public health and safety and the common defense and security." It would appear that the text acknowledges that the IMP mitigates some cyber activities. If this is true then the sentence is not needed. Delete sentence.	or supporting nuclear power plant operations. The NRC has instead revised the sentence to state: "Mitigation of opportunities for insider tampering is particularly important because an insider may know how to manipulate various systems in ways that are difficult to detect. Any acts of wrongdoing or tampering are particularly serious matters because of the potential adverse impact on nuclear power plant safety and security that could adversely affect the protection of public health and safety and the common defense and security." Based on administrative renumbering, the revised sentence now appears under Section C.1 as the first paragraph on page 9.
17. NEI	C.1.2, 1st Paragraph (Pages 8-9)	DG-5044 language: It is important to recognize that the IMP program alone does not address all cyber threats and attack vectors. As a result, the IMP alone does not take the place of other cyber security requirements and controls used to mitigate cyber attack vectors and pathways that pose a threat to equipment. NEI comment: Paragraph not portion marked. Mark paragraph as (OUO-SRI). The IMP should be provided credit for mitigating insider cyber threats and attack vectors. It does not impact outside cyber security threats and	The NRC agrees with the commenter's request to revise the phrase "mitigate cyber attack vectors" to "mitigate outside cyber attack vectors." An insider mitigation program (IMP) alone does not address all cyber threats and attack vectors. As a result, the IMP cannot take the place of other cyber security requirements and controls used to mitigate outside cyber-attack vectors and pathways that pose a threat to equipment. The NRC disagrees with the commenter's request to portion mark Section C.1.2 as OUO-SRI. Consistent with the Commission direction in the Staff Requirements Memorandum (SRM)—SECY-17-0095—Review and Approval of Proposed Revision to RG 5.77, "Insider Mitigation Program," dated July 14, 2021 (ML21195A356), the NRC staff

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		attack vectors. Differentiate between the two threats. The commenter proposed the following edits: "(OUO-SRI) It is important to recognize that the IMP program alone does not address all cyber threats and attack vectors. As a result, the IMP alone does not take the place of other cyber security requirements and controls used to mitigate outside cyber attack vectors and pathways that pose a threat to equipment."	has critically examined the designation of the document and determined that it should not be designated as "Official Use Only—Security Related Information." Based on administrative renumbering, the revision now appears under Section C.1 as the second paragraph on page 9 of DG-5044.
18. NEI	C.1.2, 1st Paragraph (Pages 8-9)	DG-5044 language: It is important to recognize that the IMP program alone does not address all cyber threats and attack vectors. As a result, the IMP alone does not take the place of other cyber security requirements and controls used to mitigate cyber attack vectors and pathways that pose a threat to equipment. NEI comment: This paragraph states that the IMP does not address all cyber threats and attack vectors. Concern: This paragraph implies that IMPs do not effectively mitigate the internal cyber threat. The result could be an interpretation that the implementation of cyber security controls within a protected or vital area must be sufficiently robust as to withstand the determined effort of an insider as though no IMP were in place. However, the "Purpose" section of DG-5044 states, "This	The NRC disagrees with the comment. Section C.1.2 makes two statements: 1) that the insider mitigation program (IMP) alone does not address all cyber-attack vectors, and 2) the IMP does not take the place of cyber security requirements and controls. The proposed amendment incorrectly states that the IMP alone mitigates the internal cyber threat. The IMP assists in the mitigation of the cyber threat, just as it does in the physical protection program, consistent with the licensee's implementation of the IMP program. Licensees must implement cyber security policies, practices, and controls to ensure that critical digital assets (CDAs) are adequately protected, as required by 10 CFR 73.54. These policies, practices and controls may not specifically be a part of a licensee's IMP. Therefore, it is not accurate to say that the IMP itself mitigates the internal cyber threat. Accordingly, the NRC has made no change to DG-5044 based on this comment.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		regulatory guide describes an approach that the staff of the U.S. Nuclear Regulatory Commission (NRC) considers acceptable for an insider mitigation program (IMP) for nuclear power reactors that contain protected or vital areas as required by Title 10 of the Code of Federal Regulations (10 CFR) 73.55(b)(9)(i)." Recommendation: The paragraph should be amended, as recommended in the suggested wording, to clarify that the IMP mitigates the internal cyber security threat. The commenter proposed to add a new third sentence to the first paragraph of Section C.1.2 that states: "The IMP mitigates the internal threat, including the internal cyber threat."	
19. NEI	C.1.2, 1st Paragraph, 4th Sentence (Page 9)	DG-5044 language: An example of this coordination is found in the need for security and human resources personnel to work closely with employee assistance program (EAP) personnel, an element of the FFD program described in 10 CFR Part 26, to ensure that individuals demonstrating any potential to harm themselves or others are reported to appropriate security personnel for evaluation as a potential insider threat, without creating the perception that seeking help via the EAP will result in adverse action. NEI comment:	The NRC agrees with this comment and has revised DG-5044 accordingly. In addition, the NRC has made minor clarifying revisions. The revised sentence states: "For example, access authorization personnel should work closely with employee assistance program (EAP) personnel, an element of the FFD program described in 10 CFR Part 26, to ensure that individuals demonstrating any potential to harm themselves or others are reported to appropriate security personnel for evaluation as a potential insider threat, without creating the perception that seeking help through the EAP will result in adverse action.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		The terms “security and human resources” should be replaced with the term “access authorization” which is the organization tasked to work with EAP and others to ensure that individuals demonstrating any potential to harm themselves or others are reported to appropriate security personnel for evaluation as a potential insider threat, without creating the perception that seeking help via the EAP will result in adverse action. The commenter proposed the following edits: “An example of this coordination is found in the need for access authorization personnel to work closely with employee assistance program (EAP) personnel, an element of the FFD program described in 10 CFR Part 26…”	Based on administrative renumbering, the revised text now appears in the fourth paragraph of Section C.1. on page 9.
20. NEI	C.1.2, 1st Paragraph, 4th Sentence (Page 9)	DG-5044 language: An example of this coordination is found in the need for security and human resources personnel to work closely with employee assistance program (EAP) personnel, an element of the FFD program described in 10 CFR Part 26, to ensure that individuals demonstrating any potential to harm themselves or others are reported to appropriate security personnel for evaluation as a potential insider threat, without creating the perception that seeking help via the EAP will result in adverse action. NEI comment: The term “human resources” has specific meaning within licensee organizations. Within many	The NRC addressed the commenter’s request to replace “security and human resources personnel” under Comment Number 19. The NRC disagrees with the commenter’s request to delete the phrase “personnel to work closely with employee assistance program.” The EAP is required under 10 CFR 26.35(c) to report to the FFD program management if they determine that an individual poses a threat to others or themselves. A licensee’s EAP may also wish to inform appropriate security personnel to help ensure adequate protection of other individuals, the facility, and the individual employee. Accordingly, the NRC has made no change to DG-5044 based on this comment.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		licensee organizations the human resources personnel are not involved. A more generalized term. In addition the term "Security" should be changed to Access Authorization. The commenter proposed the following edits: "An example of this coordination is found in the need for ~~security~~ access authorization and organizations providing support ~~personnel to work closely with employee assistance program~~ (e.g., employee assistance program (EAP) personnel, ~~an element of~~ to the FFD program described in 10 CFR Part 26, to ensure that individuals…"	
21. NEI	C.1.2, 1st Paragraph, Last sentence (Page 9)	DG-5044 language: In addition, licensee personnel should be able to recognize and report behaviors adverse to the safe operation and security of the facility, including unusual interest in security practices, security procedures, or involvement in security or operational activities outside an employee's normal work scope. NEI comment: Later in the document Section 4, DG 5044 characterizes behaviors such as "recognize and report behaviors adverse to the safe operation and security of the facility, including unusual interest in security practices, security procedures, or involvement in security or operational activities outside an employee's normal work scope," OUO-SRI. It is suggested that this paragraph be marked "OUO-SRI," the sentence be removed, or the	The NRC disagrees with the comment. The NRC has not deleted the sentence because it emphasizes the need for licensee personnel to recognize and report behaviors adverse to the safe operation and security of the facility. Having licensee personnel capable of recognizing and reporting such behavior is an essential component of an effective insider mitigation program. The NRC does not agree that this sentence should be marked as OUO-SRI or made a separate paragraph and marked OUO-SRI. Consistent with the Commission direction in Staff Requirements Memorandum (SRM)—SECY-17-0095—Review and Approval of Proposed Revision to RG 5.77, "Insider Mitigation Program," dated July 14, 2021 (ML21195A356), the NRC staff has removed all OUO-SRI portion markings from DG-5044.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		sentence be made a separate paragraph and marked OUO-SRI.	Accordingly, the NRC has made no change to DG-5044 based on this comment.
22. NEI	C.2 Applicability (Page 9)	The IMP is applicable to individuals assigned to provide defense-in-depth against identified threats or individuals. At a minimum, to mitigate the potential for an insider to be successful, and as directed by the DBT Order, EA-03-086, an IMP must consist of the following elements for all personnel with unescorted access to the protected and vital areas of a facility, or those who have been certified for unescorted access authorization: (1) a security determination (certification or unescorted access); (2) initial and random substance abuse testing; (3) psychological assessments, which may include a medical evaluation; (4) review by the immediate supervisor at least annually; and, (5) a security determination conducted by the reviewing official at the conclusion the periodic reinvestigation. For additional guidance, see RG 5.66, "Access Authorization Program for Nuclear Power Plants" In a letter dated April 5, 2004, from Roy Zimmerman (NRC) to Steven Floyd (NEI), the NRC specified that the Insider Mitigation program components were as follows: • Trained to recognize tampering • Procedures to react • Capture events in CAP and • IMP patrols	The NRC disagrees with the comment. The referenced letter provided implementation standards for the insider mitigation program (IMP) pending the initial issuance of RG 5.77. On April 29, 2003, the NRC issued NRC Order EA-03-086, "*Requiring Compliance with Revised Design Basis Threat* (DBT)." Order EA-03-086 set forth the minimum elements that a licensee's IMP must implement. A licensee may implement other elements, such as those described in the April 5, 2004, letter referenced by the commenter, to increase the effectiveness of its IMP. However, the objective of the April 5, 2004, letter was to help licensees develop standard Security Plans to achieve consistent, industry-wide implementation of the IMP requirements in the February 25, 2002, January 7, 2003, and April 29, 2003, Orders. The commenter's references to previous IMP elements found in the letter and the differences in IMP elements is an inaccurate statement. The requirements in the DBT Orders are the minimum requirements for a licensee IMP and still remain in place today. Accordingly, the NRC has made no change to DG-5044 based on this comment.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		The difference with the previous IMP's elements should be explained. The industry desires clarification on the specifics of the Insider Mitigation Program elements as compared to the 2004 letter.	
23. NEI	C.2.1 General Applicability, 1st Sentence (Page 9)	DG-5044 language: The IMP applies to all persons who are granted and/or maintain unescorted access or unescorted access authorization to an NRC licensed power reactor facility. NEI comment: For consistency with other documents a change in the ordering of the first sentence is suggested. The commenter proposed the following edits: "...The IMP applies to all persons who are certified unescorted access authorization and/or granted and/or maintain unescorted access authorization/access at an NRC-licensed power reactor facility."	The NRC agrees with the intent of the comment but has not accepted the specific revision suggested by the commenter. The NRC does not understand what the commenter means by stating, "For consistency with other documents a change in the ordering of the first sentence is suggested." However, the NRC did revise DG-5044 to state: "The IMP applies to all persons who are granted or retain unescorted access authorization to a protected or vital area." Based on administrative renumbering, the revised sentence now appears under the "General Applicability" subheading in Section C.2.
24. NEI	C.2.1 General Applicability, 2nd Sentence (Page 9)	DG-5044 language: Licensees should evaluate whether to include personnel assisting with unescorted access determinations, such as FFD program personnel and certain persons who have duties and responsibilities in the Emergency Operations Facility (EOF), as described in Section 2.3 below NEI comment: It is suggested that the paragraph be broadened and shortened. Combine the FFD Program personnel and personnel that respond to the EOF,	The NRC agrees with the intent of the comment but has not accepted the specific revision suggested by the commenter. Instead, the NRC has revised DG-5044 to state: "Licensees should evaluate whether to include personnel assisting with unescorted access determinations, such as FFD program personnel and certain persons who have duties and responsibilities in the Emergency Operations Facility, as described in Section C.2.2.3 of this RG. Insiders may occupy any position within a

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		etc., into "other personnel at the licensee's discretion." The commenter proposed the following edits: "Licensees should evaluate whether to include ~~personnel assisting with~~ ~~unescorted access determinations,~~ ~~such as FFD program personnel and~~ ~~certain persons who have duties and responsibilities in the Emergency~~ ~~Operations Facility (EOF), as~~ ~~described in Section 2.3 below~~ other personnel, at the licensee's discretion."	licensee's organization, and the IMP applies to all personnel that are in an unescorted access status or are certified for unescorted access authorization. Persons in the critical group are considered to present a greater risk as an insider threat because of their knowledge of the plant, access to vital plant equipment, access to drug and alcohol records, and authorization determinations, or because they are in possession of weapons inside the protected area of a licensed facility." Based on administrative renumbering, this revised text now appears under the "General Applicability" subheading in Section C.2, "Applicability."
25. NEI	C.2.2 The Critical Group, 1st Paragraph, Last Sentence (Page 10)	DG-5044 language: As described in 10 CFR 73.56(i)(1)(v)(B), the trustworthiness and reliability determination for any individual in the critical group must be re-established within 3 years of the date on which that determination was last made, or more frequently, based on factors determined by the licensee or applicant. At a minimum, as described in 10 CFR 73.56(i)(1)(v)(B), the current determination shall be based on a criminal history update, credit history reinvestigation, and a psychological reassessment within 3 years of the date on which these elements were last completed. NEI comment: The last sentence includes the psychological assess [sic] for a critical group member to be on a 3 year cycle. 10 CFR 73.56(i)(1)(v)(B) Maintaining	The NRC agrees with the comment and has amended DG-5044, with minor modification, to state: "At a minimum, as described in 10 CFR 73.56(i)(1)(v)(B), the current determination shall be based on a criminal history update and credit history reinvestigation within 3 years of the date on which these elements were last completed and a psychological reassessment within 5 years of the date the last psychological assessment was completed." Based on administrative renumbering, the amended text now appears in the second paragraph of Section C.2.1.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		unescorted access or unescorted access authorization states: "(B) For individuals who perform one or more of the job functions described in this paragraph, the trustworthiness and reliability determination must be based on a criminal history update and credit history reevaluation within three years of the date on which these elements were last completed, or more frequently, based on job assignment as determined by the licensee or applicant, and a psychological re-assessment within 5 years of the date on which this element was last completed." Revise the last sentence to reflect a 5-year psychological re-assessment periodicity. The commenter proposed the following edits: "At a minimum, as described in 10 CFR 73.56(i)(1)(v)(B), the current determination shall be based on a criminal history update, credit history reinvestigation within 3 years of the date on which these elements were last completed, and a psychological reassessment within 5 years of the date the last psychological assessment was completed."	
26. NEI	C.2.2 The Critical Group, Paragraph (5) (Page 10)	DG-5044 language: (5) (U) Individuals who have access to, extensive knowledge of, or administrative control over plant digital computer and communication systems and networks, as identified in 10 CFR 73.54, including: a) (U) plant network systems administrators,	The NRC agrees with the intent of the comment but has not accepted the specific revision suggested by the commenter. First, the NRC has moved all "critical group" activity descriptions under paragraph (5) of Section 2.2 to the Glossary in DG-5044. Other NRC responses

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		b) (U) IT personnel who are responsible for securing plant networks…. NEI comment: Paragraph (5) describes those individuals that should be included within the critical group for cyber security. Concern: The application of the IMP requirements for the critical group to cyber security has been challenging for the industry. The wording in 10 CFR 73.56(i)(1)(v)(B)(4) has been interpreted as: 1) Applying to ALL individuals having EITHER access OR extensive knowledge OR administrative control; and, 2) Applying to every digital asset identified in 10 CFR 73.54. The industry developed SFAQ 10-05 to address concern (1), however, concern (2) has not been addressed, and should be in this revision to RG 5.77. The impact of concern (2) has been exacerbated by the large number of digital assets (CDAs) - including many located outside of a PA or VA, or CDAs associated with SSCs in the balance of plant that were added to the scope of the cyber security rule after it was issued. NEI understands that many licensees have included very large numbers of individuals within the critical group – and given the nature of many	cover these changes in detail (Comment Numbers 27, 28, 29, and 30). Second, the NRC has added the following statement to Section 2.2: “Note: To further clarify 10 CFR 73.56(i)(1)(v)(B)(4), the term “information technology (IT) personnel” has been further defined in the glossary and is consistent with Security Frequently Asked Question (SFAQ) 10 05, “IT Functions for the Critical Group,” dated April 4, 2010 (Ref. 15).” This revised content now appears under an administratively renumbered Section 2.1 “The Critical Group.” Third, the NRC has revised Section 3.3, “Cyber Security Elements” to state: “Pursuant to 10 CFR 73.55(b)(9)(ii)(C), a licensee’s IMP must contain elements from the cybersecurity program described in 10 CFR 73.54. As required by 10 CFR 73.54(a), a licensee’s cybersecurity program must provide high assurance that digital computer and communication systems and networks are adequately protected against cyberattacks, up to and including the design-basis threat as described in 10 CFR 73.1. RG 5.71 provides guidance on the implementation of the NRC’s cybersecurity requirements and provides a framework for the identification of those digital assets that must be protected from cyberattacks. One means of complying with the requirement to include cybersecurity elements in the IMP is to ensure that the applicable cybersecurity controls

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		of the digital assets – without a commensurate increase in safety or security. Recommendation: The suggested wording provides a minor reorganization to the language in DG 5044 to address the intent of SFAQ 10-05, and adds clarity for the scope of individuals should be those who pose a real risk to the safe operation of the plant. These changes address both industry concerns. The definition should appear in the glossary and with the proposed revision: (5) (U) Individuals who have the combination of access to, ~~and~~ administrative control over, ~~or~~ and contain extensive knowledge of, plant digital computer and communication systems and networks, as identified in 10 CFR 73.54, associated with the safety related systems of the plant….	identified in RG 5.71 are applied to the digital computer and communication systems and networks routinely used by members of the critical group, particularly IT personnel. The glossary of this RG defines "critical group" and "information technology (IT) personnel" as the terms are used in 10 CFR 73.56(i)(1)(v)(B). These definitions are consistent with those given in SFAQ 10-05. By establishing, maintaining, and successfully integrating these security controls into a site-specific cybersecurity program and referencing these controls in the IMP, the licensee can provide assurance of an effective IMP."
27. NEI	C.2.2 The Critical Group, Note, (iv) and (v) (Page 11)	DG-5044 language: iv. (U) Individuals assigned any duty to search for contraband (e.g., weapons, explosives, or incendiary devices). v. (U) Individuals qualified for and assigned duties as: armed security officers, armed responders, alarm station operators, response team leaders, and armorers. NEI comment: Paragraphs (5)(iv) and (5)(v) should be numbered	The NRC agrees with the intent of the comment but has not accepted the specific revisions suggested by the commenter. The NRC agrees that renumbering (iv) and (v) would clarify that these activities do not apply to IT personnel, but the NRC has chosen alternative approaches to resolve this comment. First, the content of (iv) already appears in the "Glossary" under the definition for "critical group", paragraph c. Therefore, the NRC has eliminated paragraph (5)(iv) from the revised "Critical Group"

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		section 2.2 paragraphs (6) and (7), respectively. 2.2 (6) and 2.2 (7), respectively.	section of DG-5044, which has been administratively renumbered as Section C.2.1. Second, all the classes of individuals identified in paragraph (5)(v) (i.e., armed security officers, armed responders, alarm station operators, response team leaders, and armorer) are captured within the scope of paragraph a in the "Critical Group" definition in the Glossary of DG-5044. The relevant section of the definition states: "a. has extensive knowledge of facility defensive strategies or designs and/or implements the plant's defense strategies."
28. NEI	C.2.2 The Critical Group, 2nd Paragraph, (5) (Page 10)	DG-5044 language: (U) Individuals who have access to, extensive knowledge of, or administrative control over plant digital computer and communication systems and networks, as identified in 10 CFR 73.54, including: NEI comment: **Note I, first paragraph** (U) an individual who has the combination of electronic access AND the administrative control (e.g., "system administrator" rights) to alter one or more security controls associated with one or more critical digital assets. The 2.2(5) paragraph and the Note I, first paragraph are the describing the same set of individuals. It is suggested that the paragraphs be combined.	The NRC agrees with the intent of the comment to combine the content of paragraph (5) and the first paragraph of "i" that appears under "Note". However, the NRC has not accepted the commenter's edits. Instead, the NRC has chosen to move, combine, and revise this information as part of a new definition for "information technology (IT) personnel" added to the Glossary in DG-5044. The definition of "information technology (IT) personnel" states: "1) Any individual who has the combination of electronic access AND the administrative control (e.g., "system administrator" rights) to alter one or more security controls associated with one or more CDAs should be in the critical group. A person with administrative control has the electronic access and rights to independently change either the

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		The commenter proposed the following edits: "(U) Individuals who have a combination of extensive knowledge and administrative control over plant digital computer and communication systems and networks (e.g. "system administrator rights") to alter one or more security controls associated with one or more critical digital assets, as identified in 10 CFR 73.54, including:"	configuration of a CDA or the cybersecurity controls in place for a CDA, in a manner that could result in an adverse impact to SSEP functions…."
29. NEI	C.2.2 The Critical Group, Note, i, 2nd Paragraph (Pages 10-11)	DG-5044 language: (U) Administrative control: A person with administrative control has the electronic access and rights to independently change either the configuration of a critical digital asset (CDA) or the cyber security controls in place for a CDA in a manner that could result in an adverse impact to Safety, Important to Safety, Security or Emergency Preparedness (SSEP) functions. NEI comment: This appears to be a definition of Administrative Control. Consider moving the definition to the document's Glossary. The commenter proposed the following edits: "**Administrative control:** the electronic access and rights to independently change either the configuration of a critical digital asset (CDA) or the cyber security controls in place for a CDA in a manner that could result in an adverse impact to Safety, Important to Safety, Security or Emergency Preparedness (SSEP) function..."	The NRC agrees with the comment and has revised, with minor modification, and moved the administrative control statement to the existing definition for "critical group" in the Glossary of DG-5044. The statement appears under paragraph e. The NRC also included the administrative control statement, with minor modification, as part of a new definition of "information technology (IT) personnel" that appears in the Glossary in DG-5044. The second sentence in the first paragraph of the definition states: "…A person with administrative control has the electronic access and rights to independently change either the configuration of a CDA or the cybersecurity controls in place for a CDA, in a manner that could result in an adverse impact to SSEP functions…."

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
30. NEI	C.2.2 The Critical Group, Note, ii (Page 11)	DG-5044 language: (ii) (U) An individual with extensive knowledge of the site-specific cyber-defensive strategy. Extensive knowledge is defined as having: (U) a. (U) knowledge of the cyber security controls in place for a CDA; b. (U) knowledge of how the configuration of a CDA or the cyber security controls can be modified or leveraged in a manner that could result in an adverse impact to SSEP functions; c. (U) knowledge of vulnerabilities of the site specific cyber security defensive strategy. NEI comment: This appears to be a definition of Extensive knowledge. Consider moving the definition to the document's Glossary.	The NRC agrees with the comment and has revised DG-5044 accordingly. The NRC made minor clarifying revisions and moved the extensive knowledge information to a new definition for "information technology (IT) personnel" in the Glossary of DG-5044. The second paragraph of the definition states: "(2) Any individual with extensive knowledge of the site-specific cyber defensive strategy should also be in the critical group. "Extensive knowledge" is defined as having (a) knowledge of the cybersecurity controls in place for a CDA, or (b) knowledge of how the configuration of a CDA or the cybersecurity controls can be modified or leveraged in a manner that could result in an adverse impact to SSEP functions, or (c) knowledge of vulnerabilities of the site-specific cybersecurity defensive strategy."
31. NEI	C.2.3.2 d (Page 12)	DG-5044 language: Persons, including the Medical Review Officer and site nurse or medical practitioner, if assigned, who: NEI comment: SFAQ 12-09 limits the MRO to occasions when the Medical Review officer is on site. The proposed text does not seem to recognize this understanding. The commenter proposed the following edits: "Persons, including the Medical Review Officer,	The NRC agrees with the intent of the comment but has not accepted the specific revision suggested by the commenter. Instead, the NRC has revised the sentence to state: "d. persons, including the Medical Review Officer, site nurse, or medical practitioner, when on site, who do the following…" Based on administrative renumbering, the revised text appears in Section C.2.2.2 d.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		when onsite, and site nurse or medical practitioner, if assigned…"	
32. NEI	C.2.3.3 (Page 12)	DG-5044 language: (U) The IMP should apply to persons designated to physically report to the EOF and those persons who may have unmonitored access to sensitive (e.g. security- or safety-related) information. NEI comment: Placing persons under IMP beyond those required by regulation such as persons who may have unmonitored access to sensitive information (e.g., security safety related information) is ambiguous without definition or regulatory basis. The commenter proposed the following edits: "Provide a reference to other Regulatory Guidance or Policy Issue (e.g., RG-5.79 Protection of Safeguards Information, SECY-04-0191, Withholding Sensitive Unclassified Information Concerning Nuclear Power Reactors From Public Disclosure, etc.)"	The NRC disagrees with the comment. There is no regulatory requirement to apply the insider mitigation program to individuals who report to the Emergency Operations Facility (EOF) or who have access to sensitive security or safety related information, unless those individuals are part of the Critical Group or they could remotely take actions by electronic means remotely that could adversely impact the licensee's operational safety, security, or emergency preparedness. These individuals are already covered by existing regulatory requirements. Licensees should be aware of the existing guidance applicable to these individuals and situations. This paragraph is suggesting that a licensee may wish to extend its IMP program to individuals who are not covered by existing regulatory requirements. There is no need to reference guidance or policy when a licensee elects to extend the scope of its IMP beyond what is regulatorily required. Accordingly, the NRC has made no change to DG-5044 based on this comment.
33. NEI	C.3.1.1.2, Last Sentence (Page 13)	DG-5044 language: (OUO-SRI) … Licensees shall, as required in 10 CFR 26.189, consider the potential insider threat when making FFD determinations. NEI comment: 10 CFR 26.189 does not contain this requirement.	The NRC agrees with the comment and has amended the sentence, with minor modification, to state: "Licensees should consider the potential insider threat when making FFD determinations under 10 CFR 26.189(c)(2).

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		Consider adding the suggested text. The commenter proposed the following text addition: "Licensees should consider the potential insider threat when making FFD determinations as required in 10 CFR 26.189(c)(2), (e.g., Licensee or other entity management personnel shall implement the required actions to ensure any possible limiting condition does not represent a threat to workplace or public health and safety.)"	For example, licensee or other entity management personnel should implement the required actions to ensure any potential limiting condition does not represent a threat to workplace or public health and safety." Based on administrative renumbering, the revised text now appears under Section C.3.1.1.5. The NRC staff also removed the "(OUO-SRI)" portion marking from this paragraph, consistent with the Commission direction in the Staff Requirements Memorandum (SRM)—SECY-17-0095—Review and Approval of Proposed Revision to RG 5.77, "Insider Mitigation Program," dated July 14, 2021 (ML21195A356).
34. NEI	C.3.1.2 Behavioral Observation, § 26.33, 2nd Sentence (Page 13)	DG-5044 language: Behavioral observation is performed by individuals trained under § 26.29 to detect behaviors that may indicate possible use, sale, or possession of illegal drugs; use or possession of alcoholic beverages, or impairment from fatigue or any cause that, if left unattended, may constitute a risk to public health and safety or the common defense and security. NEI comment: The concept of "Behavioral Observation" is broader than the [sic] in Section 3.1.2 of the draft RG. The term encompasses other undesirable behaviors that an individual may display in the nuclear power plant environment. It is suggested that in this context that the paragraph 3.1.2 text be changed.	The NRC agrees with the comment and has amended DG-5044, with minor modification, to state: "Although behavioral observation includes the early identification of many other behaviors that may pose a risk to a nuclear power plant or spent fuel pool, it is performed by individuals trained under 10 CFR 26.29, "Training," to detect behaviors that may indicate possible use, sale, or possession of illegal drugs; use or possession of alcohol; or impairment from fatigue or any cause that, if left unattended, may constitute a risk to public health and safety or the common defense and security."

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		The commenter proposed the following edits: "Although behavioral observation includes the early identification of many other behaviors that may pose a risk to a nuclear power plant, it is performed by individuals trained under § 26.29 to detect behaviors that may indicate possible use, sale, or possession of illegal drugs; use or possession of alcoholic beverages, or impairment from fatigue or any cause that, if left unattended, may constitute a risk to public health and safety or the common defense and security."	
35. NEI	C.3.1.2 Behavioral Observation, § 26.33, Last sentence (Page 13)	DG-5044 language: Implementing these requirements helps provide high assurance of an effective behavioral observation program at operating and decommission power. NEI comment: The industry suggests removal of this section and to include the section within a separate decommissioning rulemaking. The commenter proposed the following edits: "Implementing these requirements helps provide high assurance of an effective behavioral observation program at operating ~~and decommission~~ power."	The NRC disagrees that guidance on implementing insider mitigation programs at decommissioning reactors should be removed from DG-5044. However, the NRC has revised Section C.3.1.2 to include "or spent fuel pool," as well as other minor clarifying revisions. The first three sentences of the first paragraph under Section 3.1.2 in the revised DG-5044 state: "Licensees and other affected entities must ensure that the individuals who are subject to 10 CFR Part 26, Subpart B, "Program Elements," are also subject to a behavioral observation program that meets the requirements specified in 10 CFR 26.33, "Behavioral observation," and 10 CFR 73.56(f). Although behavioral observation includes the early identification of many other behaviors that may pose a risk to a nuclear power plant or spent fuel pool, it is performed by individuals trained under 10 CFR 26.29, "Training,"

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
			to detect behaviors that may indicate possible use, sale, or possession of illegal drugs; use or possession of alcohol; or impairment from fatigue or any cause that, if left unattended, may constitute a risk to public health and safety or the common defense and security. Further, individuals should be trained in recognizing and reporting behaviors as required in 10 CFR 73.56(f), which may be considered adverse to the safe operation and security of the licensee facility." The NRC has adopted a graded approach to security requirements at reactors that is commensurate with the reductions in radiological risk at four levels of decommissioning: (1) permanent cessation of operations and removal of all fuel from the reactor vessel, (2) sufficient decay of fuel in the spent fuel pool such that it would not reach ignition temperature within 10 hours under adiabatic heat up conditions, (3) transfer of all fuel to dry storage, and (4) removal of all fuel from the site. Until the licensee removes all irradiated fuel from the spent fuel pool implementing an Insider Mitigation Program is required. In addition, the NRC response to Comment Number 3 discusses the ongoing decommissioning rulemaking, which is proposing revisions to 10 CFR Part 26 and the insider mitigation program.
36. NEI	C.3.2.1 Initial Security Determination (Pages 13-14)	DG-5044 language: Initial security measures for completing background investigations and other programmatic elements required by the NRC,	The NRC agrees with the comment and has revised DG-5044 accordingly.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		through the implementation of the requirements of 10 CFR 73.56 and 10 CFR 73.57 and the latest NRC staff endorsed guidance of NEI 03-01, provide high assurance that persons initially selected for unescorted access or unescorted access authorization are trustworthy and reliable and do not present a risk to public health and safety or the common defense and security. NEI comment: For consistency with other documents a change in the ordering of the first sentence is suggested. The commenter proposed the following edits: "...the latest NRC staff endorsed guidance of NEI 03-01, provide high assurance that persons initially certified for unescorted access authorization or granted unescorted access are trustworthy and reliable and do not present a risk to public health and safety or the common defense and security."	In addition, the NRC has replaced the phrase "the latest NRC staff endorsed guidance of NEI 03-01" with "consistent with guidance contained in RG 5.66". NEI 03-01, while endorsed by the NRC staff, is not a document authored by the NRC. The revised sentence states: "Initial security measures for completing background investigations and other programmatic elements required by the NRC, through the implementation of the requirements of 10 CFR 73.56 and 10 CFR 73.57 and consistent with guidance contained in RG 5.66, provide high assurance that persons initially certified for unescorted access authorization or granted unescorted access are trustworthy and reliable and do not present a risk to public health and safety or the common defense and security."
37. NEI	C.3.2.2.1, 1st Sentence (Page 14)	DG-5044 language: Initial psychological assessments should ensure that any testing mechanism applied, in whole or in part, to a psychological determination of suitability for unescorted access includes the opportunity to detect the need for a medical evaluation as described in paragraph (c) below. NEI comment: The reference to "paragraph c below" seems to refer to the paragraph numbering system in RG 54.77. The same numbering did not flow	The NRC agrees with the intent of the comment but has not accepted the specific revision suggested by the commenter. Instead, the NRC deleted the phrase "as described in paragraph (c) below" and moved the revised sentence to a renumbered Section C.3.2.2.1 b.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		through to the draft 5044 document. It is now the 3rd bullet. The commenter proposed the following edit: "Initial psychological assessments should ensure that any testing mechanism applied, in whole or in part, to a psychological determination of suitability for unescorted access includes the opportunity to detect the need for a medical evaluation as described in 3.2.2.3 below."	
38. NEI	C.3.2.2.2 (Page 14)	DG-5044 language: Before any psychological or medical assessment, the appropriate practitioner should review a current position description for the person being interviewed and the most recently completed supervisory review, if applicable, for information that could assist the physician practitioner in his or her assessment. NEI comment: The word "physician" should be replaced with the word "appropriate."	The NRC agrees with this comment and has replaced the word "physician" with the word "appropriate." Based on administrative renumbering, the revised paragraph now appears under Section C.3.2.2.1 a.
39. NEI	C.3.2.2.2, 3rd Bulleted Paragraph, 3rd Sentence (Page 14)	DG-5044 language: Medical evaluations triggered by a psychological recommendation should include a review of the individual's prescribed medications to ensure that these medications do not impair the person's judgment to the extent that trustworthiness and reliability are jeopardized. Individuals identified as candidates for further medical review should be referred to a physician for further evaluation. NEI comment:	The NRC agrees with the comment and has revised DG-5044 to include the commenter's suggested language, with minor modification. The NRC also included "(see 10 CFR 26.189, "Determination of fitness)" to the end of the sentence to clarify the regulatory requirement applicable to the "further evaluation" phrase. The revised sentence states: "Individuals identified as candidates for further medical review should be referred to a physician

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		The term physician should be qualified to include a physician who may be the MRO. The commenter proposed the following edits: "…Individuals identified as candidates for further medical review should be referred to a physician, who may be the MRO, for further evaluation."	who may be qualified as the Medical Review Officer, for further evaluation (see 10 CFR 26.189, "Determination of fitness")." Due to an administrative change in numbering, this sentence appears under Section C.3.2.2.4.
40. NEI	C.3.2.3 Annual review by Immediate Supervisor, 2nd Paragraph (Page 15)	DG-5044 language: A review conducted by the assigned supervisor has value as an integral part of the behavior observation program (BOP) required by 10 CFR 73.56(i)(1)(iv). This review creates a platform for interaction between the supervisor and the employee to the extent that the supervisor has the opportunity to become cognizant of any condition that may cause the employee to act or behave in an unconventional manner. In addition, the supervisory review provides an opportunity for the supervisor to consider whether any circumstances may indicate the need to refer the employee for additional medical or psychological review. The annual supervisory review or interview must incorporate the consideration of any self-reporting as required in 10 CFR 73.56(g). NEI comment: The paragraph does not address the immediate reporting required of such individuals. Individuals are required to self-report legal actions in accordance with licensee procedures. An effective program does not wait for an annual supervisory review to report legal actions. The actions are	The NRC agrees with the portion of the comment stating that individuals, consistent with the requirement in 10 CFR 73.56(g), must promptly report any legal actions taken by law enforcement or a court of law. The NRC disagrees with the commenter's request to delete this statement in Section C.3.2.3 because it reminds licensees that the annual supervisory review conducted as required in 10 CFR 73.56(i)(1)(iv) should take into consideration any information obtained by the licensee as a result of an individual's compliance with the self-reporting requirement in 10 CFR 73.56(g). Consideration of such information is valuable to licensee supervisors that conduct the comprehensive annual reviews. The NRC did make one change in Section C.2.3.2, replacing "must" with "should" in the phrase "review or interview must incorporate". The revised sentence states: "The annual supervisory review or interview should incorporate the consideration of any self-reporting as required in 10 CFR 73.56(g)."

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		report [sic] timely to the licensee reviewing official who evaluates the matter in terms of the licensee denial criteria. Re-submitting the legal action or other behavior on an "Annual Supervisory Review" is duplicate work and the review's information is already known to the licensee Reviewing Official. Delete.	
41. NEI	C.3.2.3.1 Last sentence (Page 16)	DG-5044 language: In some cases, the supervisor may not have frequent enough personal interaction with the individual throughout the review period needed to develop an informed and reasonable opinion regarding the individual's behavior, trustworthiness, and reliability. When this unusual condition occurs, the interview may consist of face to face contact, in addition to gathering of information from personnel who have had frequent interaction with the individual, combined with other documented methods of trustworthiness and reliability. In addition, the licensee must ensure that the annual supervisory review or interview is conducted consistent with the requirements of 10 CFR 26.27, "Written Policy and Procedures," and 10 CFR 26.29, "Training." NEI comment: The last sentence of the paragraph does not seem to modify the paragraph's main message that a supervisor who does not have frequent enough interactions to perform the Annual Supervisory Review has other options. It introduces another topic that the Annual Supervisory Review must be consistent with 10 CFR 26.17 and 10 CFR 26.29	The NRC agrees with the comment and has deleted the sentence: "In addition, the licensee must ensure that the annual supervisory review or interview is conducted consistent with the requirements of 10 CFR 26.27, "Written Policy and Procedures," and 10 CFR 26.29, "Training."

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		which talk to self-reporting of legal actions and its attendant training respectively. In addition, the suggestion is to remove the last sentence as 10 CFR 26.27 and 29 [sic] does not require the Annual Supervisory Review.	
42. NEI	C.3.2.3.2 Last Sentence (Page 16)	DG-5044 language: This review serves two purposes. First, it can identify issues related to physical or mental impairment that fall under the general performance objectives of 10 CFR Part 26. Second, it can identify issues related to trustworthiness and reliability other than those related to physical or mental impairment. NEI comment: The last sentence contradicts the BOP program emphasis of immediate reporting. Recommend deleting the sentence from the document. Licensee programs require immediate reporting of observations and changes in behavior. Delete.	The NRC disagrees with the comment. The sentence does not contradict the requirement for the immediate reporting of observations and changes in behavior under the behavioral observation program (BOP). It simply states that issues related to trustworthiness and reliability are not limited solely to issues of physical and mental impairment identified by the BOP. In context, it indicates that such other trustworthiness and reliability information can be incorporated into the annual supervisory review. Accordingly, the NRC has made no change to DG-5044 based on this comment.
43. NEI	C.3.2.4 Periodic Reinvestigation of Security Determination, 2nd Paragraph, 2nd Sentence (Page 16)	DG-5044 language: (OUO-SRI) … Members of the critical group must also get a psychological reassessment within 5 years of the date on which this assessment was last completed. NEI comment: This sentence should be deleted from this paragraph as it is already contained with Section 3.2.2.2, paragraph 5 on page 15.	The NRC agrees with the comment and has revised DG-5044 accordingly. Based on administrative renumbering, the revised paragraph appears under Section 3.2.4.2 in DG-5044. The NRC staff also removed the “(OUO-SRI)” portion marking from this section, consistent with the Commission direction in the Staff Requirements Memorandum (SRM)—SECY-17-0095—Review and Approval of Proposed Revision

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		The commenter proposed the following edits: "(OUO-SRI) Under 10 CFR 73.56(i)(1)(v)(B)(1) through (5), members of the critical group must be reinvestigated within 3 years of the date on which the criminal history update and credit history reevaluation were last completed, or more frequently, based on job assignment as determined by the licensee or applicant. ~~Members of the critical group must also get a psychological reassessment within 5 years of the date on which this assessment was last completed.~~ The requirements of this section apply to all individuals with unescorted access authorization or unescorted access that are members of the critical group.…"	to RG 5.77, "Insider Mitigation Program," dated July 14, 2021 (ML21195A356).
44. NEI	C.3.2.4 Periodic Reinvestigation of Security Determination, 2nd Paragraph, 3rd Sentence (Page 16)	DG-5044 language: (OUO-SRI) … The requirements of this section apply to all individuals with unescorted access authorization or unescorted access who are members of the critical group. Individuals who have not satisfied the reinvestigation requirements shall have unescorted access authorization or unescorted access administratively withdrawn until the reinvestigation has been completed, or the worker should be reassigned to non critical group positions until the required critical group reassessment can be completed. NEI comment: It is suggested that the wording be changed for consistency. In addition consider added [sic] a second paragraph to this section to provide a recognition that all workers not deemed Critical Group are reinvestigated every five (5) years.	The NRC agrees with the comment and has amended DG-5044, with minor modification, to state: "The requirements of this section apply to all individuals certified for unescorted access authorization or granted unescorted access who are members of the critical group. As required by 10 CFR 73.56(i)(1)(vi), individuals who have not satisfied the reinvestigation requirements shall have unescorted access authorization or unescorted access administratively withdrawn until the reinvestigation has been completed, or the worker should be reassigned to non-critical group positions until the required critical group reassessment can be completed. In addition, any individual not assigned to the Critical Group is reinvestigated within 5 years of the date on which

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		The commenter proposed the following edits: "The requirements of this section apply to all individuals certified ~~with~~ unescorted access authorization or granted unescorted access who are members of the critical group. Individuals who have not satisfied the reinvestigation requirements shall have unescorted access authorization or unescorted access administratively withdrawn until the reinvestigation has been completed, or the worker should be reassigned to non-critical group positions until the required critical group reassessment can be completed. In addition, any individual not assigned to the Critical Group is reinvestigated within 5 years of the date on which the criminal history update and re-evaluation elements were last completed."	the criminal history update and re-evaluation elements were last completed." Based on administrative renumbering, the revised text appears under Section C.3.2.4.2 in DG-5044. The NRC staff also removed the "(OUO-SRI)" portion marking from this section, consistent with the Commission direction in the Staff Requirements Memorandum (SRM)—SECY-17-0095—Review and Approval of Proposed Revision to RG 5.77, "Insider Mitigation Program," dated July 14, 2021 (ML21195A356).
45. NEI	C.3.2.4 Periodic Reinvestigation of Security Determination, 3rd Paragraph, 1st Bullet, 2nd Sentence (Page 16)	DG-5044 language: Licensees should prioritize fingerprint requests to ensure there are no unanticipated staffing issues. NEI comment: This sentence should be deleted as it is no longer reflects service problems. The fingerprints are now received within a 24-hour window after submission. The commenter proposed the following edits: "…A review of criminal history records obtained under 10 CFR 73.56(d)(7) and 10 CFR 73.57, or as the Commission may require, or as Federal statutes may direct. Licensees should compare data returned from the criminal history records	The NRC disagrees with the comment. The guidance is appropriate because extenuating circumstances have sometimes prevented a timely response to requests for obtaining and processing of fingerprints that have resulted in delayed response times. This language is a reminder to licensees that processing of fingerprints should be a priority. Accordingly, the NRC has made no change to DG-5044 based on this comment.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		check with the access authorization records of the person named in the record to ensure that the person has complied with the self reporting requirements in 10 CFR 73.56(g). ~~Licensees should prioritize fingerprint requests to ensure there are no unanticipated staffing issues.~~"	
46. NEI	C.3.2.4 Periodic Reinvestigation of Security Determination, 3rd Paragraph, 2nd Bullet, 2nd Sentence (Page 16)	DG-5044 language: The individual should complete new consent to screen and Federal Credit Reporting Act disclosure and authorization statement forms before initiating this reinvestigation. NEI comment: The term Federal Credit Reporting Act should be "Fair Credit Reporting Act."	The NRC agrees with the comment and has revised DG-5044 accordingly. This discussion has been administratively renumbered as Section C.3.2.4.2 b.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
47. NEI	C.3.2.4 Periodic Reinvestigation of Security Determination, 3rd Paragraph, 3rd Bullet (Page 16)	DG-5044 language: Licensees shall take appropriate action if disqualifying information is discovered during any reinvestigation review. NEI comment: The term utilized throughout of [sic] industry document is potentially disqualifying information with the acronym (PDI). In addition, the requirement is to review the PDI against denial criteria and to take appropriate action consistent with the licensee access authorization program policies and procedures. Suggest the following word change to the text of DG-5044. The commenter proposed the following edits: "…Licensees shall review any ~~take appropriate action if~~ potentially disqualifying information (PDI) developed during a reinvestigation against the licensee's program policies and procedures and take action as appropriate ~~is discovered during any reinvestigation review~~."	The NRC agrees with the comment and has revised DG-5044, with minor modification, to state: "Licensees shall review any potentially disqualifying information during a reinvestigation against the licensee's program policies and procedures and act as appropriate." This discussion has been administratively renumbered as Section C.3.2.4.2 c.
48. NEI	C.3.2.5 Access to Vital Areas, 1st Paragraph, 2nd Sentence (Page 17)	DG-5044 language: The rule requires that access authorization lists will be updated and reapproved at least every 31 days to minimize insider threats by ensuring that personnel listed have a continued need to access vital areas to perform their official duties and not just a possibility of needing access sometime in the future. NEI comment: SFAQ 14-03, Vital Area Review, provided further agree-upon clarification of the "no less frequently	The NRC disagrees with the comment. SFAQ 14-03 clarified that licensee reviews need not be conducted at an exact 31-day interval, but that the licensee's cognizant manager or supervisor conduct a review no less frequently than every 31 days, and that there be no less than 12 reviews during each calendar year. As stated, in part, in SFAQ 14-03: "The composite list concept meets the intent of 10 CFR 73.56(j) provided that the cognizant manager/supervisor responsible for compiling each supporting list reviews, re-approves, and identifies any required changes

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		than every 31 days" rule text. The SFAQ concluded that: … The composite list would be completed each calendar month during the calendar year to meet the intent of 10 CFR 73.56 (j). This process would reduce the administrative burden on licensees when working with multiple supporting lists independently of each other. The composite list would be completed as described, to encompass no less than 12 reviews each calendar year (without counting 31 days from completion of the process from month-to-month) to meet the intent of 10 CFR 73.56(j). The suggestion is to place an asterisk (*) after 31 day and place a Note in the body of the text following the end of the paragraph. The commenter proposed the following edits: "The rule requires that access authorization lists will be updated and reapproved at least every 31 days * to minimize insider threats by ensuring that personnel listed have a continued need to access vital areas to perform their official duties and not just a possibility of needing access sometime in the future. * The composite 31-day list would be completed as described, to encompass no less than 12 reviews each calendar year (without counting 31 days from completion of the process from month—to-month) to meet the intent of 10 CFR 73.56 (j)."	for individuals as needed when the cognizant manager/supervisor directs their work activities." Accordingly, the NRC has made no change to DG-5044 based on this comment.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
49. NEI	C.3.2.5 Access to Vital Areas, 2nd Paragraph, 1st Sentence (Page 17)	DG-5044 language: The intent of this requirement is to minimize insider threats by reducing the number of individuals having unescorted vital area access, and by limiting vital area access to those personnel who specifically require access to vital areas in order to perform their duties. NEI comment: It is suggested that those required to respond to emergency conditions also be included. Often time this will increase the numbers of personnel because normal conditions may not require access but emergency conditions may. The commenter proposed the following edits: "The intent of this requirement is to minimize insider threats by reducing the number of individuals having unescorted vital area access, and by limiting vital area access to those personnel who specifically require access to vital areas in order to perform their duties, including responding to emergency conditions."	The NRC disagrees with the comment. Individuals required to respond to emergency conditions fall within the scope of personnel who require access to vital areas in order to perform their duties. Therefore, the language suggested by the commenter is not necessary. The NRC further notes that the role of emergency responders is discussed in Section C.3.2.5. Accordingly, the NRC has made no change to DG-5044 based on this comment.
50. NEI	C.3.2.5 Access to Vital Areas, 1st Paragraph (Page 17)	NEI comment: SFAQ 14-03, Vital Area Review, provided further agree-upon clarification of the "no less frequently than every 31 days" rule text. The SFAQ concluded that: …The composite list would be completed each calendar month during the calendar year to meet the intent of 10 CFR 73.56 (j). This process would reduce the administrative burden on licensees when working with multiple supporting lists independently of each other. The composite list	The NRC disagrees with the comment, which is essentially the same as Comment Number 48. Accordingly, the NRC reiterates its response to Comment Number 48 here and has made no change to DG-5044 based on this comment.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		would be completed as described, to encompass no less than 12 reviews each calendar year (without counting 31 days from completion of the process from month-to-month) to meet the intent of 10 CFR 73.56 (j). The suggestion is to place an asterisk (*) after 31 day and place a Note in the body of the text following the end of the paragraph. The commenter proposed the following edits: "The intent of this requirement is to minimize insider threats by reducing the number of individuals having unescorted access no less frequently than at a 31 day frequency *. The NRC recognizes that a single licensee manager or supervisor would not have oversight and control of every person with unescorted access to any or all of a licensee's vital areas. * The composite 31-day list would be completed as described, to encompass no less than 12 reviews each calendar year (without counting 31 days from completion of the process from month-to-month) to meet the intent of 10 CFR 73.56 (j)."	
51. NEI	C.3.2.5.1, 3rd Sentence (Page 17)	DG-5044 language: Personnel who fall into this emergency response category must be evaluated for continued need for access during the 31 day review by a cognizant licensee or applicant manager or supervisor who would be responsible for directing the work activities of the individual while that individual is present at the licensee or applicant site.	The NRC disagrees with the comment, which is essentially the same as Comment Number 48. Accordingly, the NRC reiterates its response to Comment Number 48 here and has made no change to DG-5044 based on this comment.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		NEI comment: SFAQ 14-03, Vital Area Review, provided further agree-upon clarification of the “no less frequently than every 31 days” rule text. The SFAQ concluded that: …The composite list would be completed each calendar month during the calendar year to meet the intent of 10 CFR 73.56 (j). This process would reduce the administrative burden on licensees when working with multiple supporting lists independently of each other. The composite list would be completed as described, to encompass no less than 12 reviews each calendar year (without counting 31 days from completion of the process from month—to—month) to meet the intent of 10 CFR 73.56 (j). The suggestion is to place an asterisk (*) after 31 day and place a Note in the body of the text following the end of the paragraph. The commenter proposed the following edits: “Personnel who fall into this emergency response category must be evaluated for continued need for access during the 31 day review * by a cognizant licensee or applicant manager or supervisor who would be responsible for directing the work activities of the individual while that individual is present at the licensee or applicant site. * The composite 31-day list would be completed as described, to encompass no less than 12	

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		reviews each calendar year (without counting 31 days from completion of the process from month—to-month) to meet the intent of 10 CFR 73.56 (j)."	
52. NEI	C.3.3 Cyber Security Elements (Pages 17-18)	NEI comment: Section 3.3 provides cyber security elements of an acceptable IMP. Concern: This section, in its entirety, is disjointed with the other subsections of Section 3. As written, the section appears to indicate that the controls listed be implemented in a manner sufficiently robust as to withstand the determined effort of an insider as though no IMP were in place. Recommendation Section 3.3 should be removed in its entirety, or, if retained, be replaced in its entirety with the suggested wording. The commenter proposed the following edits: "3.3 Cyber Security Elements (u) (U) The following elements support mitigation of the cyber insider threat. 3.3.1 (U) Any individual whose duties and responsibilities permit the individual to take actions by electronic means, either on site or remotely, that could adversely impact the licensee's or applicant's operational safety, security, or emergency preparedness are subject	The NRC disagrees with the commenter's request to delete Section C.3.3 of DG-5044 in its entirety. Section C.3.3 reminds licensees to be cognizant of the potential cyber threat that an insider may pose. The NRC has determined that it is more appropriate to maintain the reference to RG 5.71 but not to include the specific cyber security controls described in RG 5.71. To accomplish the intent of this section more effectively, the NRC has revised Section C.3.3. to read as follows: "Pursuant to 10 CFR 73.55(b)(9)(ii)(C), a licensee's IMP must contain elements from the cybersecurity program described in 10 CFR 73.54. As required by 10 CFR 73.54(a), a licensee's cybersecurity program must provide high assurance that digital computer and communication systems and networks are adequately protected against cyberattacks, up to and including the design-basis threat as described in 10 CFR 73.1. RG 5.71 provides guidance on the implementation of the NRC's cybersecurity requirements and provides a framework for the identification of those digital assets that must be protected from cyberattacks. One means of complying with the requirement to include cybersecurity elements in the IMP is to ensure that the applicable cybersecurity controls

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		to an access authorization program [10 CFR 73.56(b)(1)(ii)]. 3.3.2 (U) Individuals performing the job functions described in 10 CFR 73.56(i)(1)(v)(B)(4) are added to the critical group. 3.3.3 (U) Appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities. [10 CFR 73.54(d)(1)] 3.3.4 (U) Policies and implementing procedures for incident response and recovery for cyber attacks are developed and maintained. [10 CFR 73.54(e)(2) and 10 CFR 73.54(f)]"	identified in RG 5.71 are applied to the digital computer and communication systems and networks routinely used by members of the critical group, particularly IT personnel. The glossary of this RG defines "critical group" and "information technology (IT) personnel" as the terms are used in 10 CFR 73.56(i)(1)(v)(B). These definitions are consistent with those given in SFAQ 10-05. By establishing, maintaining, and successfully integrating these security controls into a site-specific cybersecurity program and referencing these controls in the IMP, the licensee can provide assurance of an effective IMP."
53. NEI	C.3.3 Cyber Security Elements (Page 18)	DG-5044 language: (OUO-SRI) Licensees should conduct random patrols, by trained staff, of CDAs that affect SSEP functions to look for obvious signs of cyber related tampering. NEI comment: The final paragraph of Section 3.3 describes that licensees should conduct random patrols of CDAs. Concern: 10 CFR 73.55(f)(2) requires licensees consider cyber attacks in the development and identification of target sets. 10 CFR 73.55(i)(5) provides a series of requirements for surveillance, observation, and monitoring, including	This is essentially the same comment as Comment Number 52. Accordingly, the NRC reiterates its response to Comment Number 52 here. The NRC staff removed the "(OUO-SRI)" portion marking from this section, consistent with the Commission direction in the Staff Requirements Memorandum (SRM)—SECY-17-0095—Review and Approval of Proposed Revision to RG 5.77, "Insider Mitigation Program," dated July 14, 2021 (ML21195A356).

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		requirements for the recognition of obvious indications of tampering. Notably, 10 CFR 73.55(i)(5)(vi) requires licensees provide random patrols of all accessible areas containing target set equipment. 10 CFR 73.55(i)(5)(vii) requires security personnel be trained to recognize obvious indications of tampering consistent with their assigned duties and responsibilities. Given the current requirements for patrols provided in 10 CFR 73.55, the net safety and security benefit from specific patrols of all CDAs is questionable. Recommendation: The final paragraph from section 3.3 should be deleted.	
54. NEI	C.3.3.1 Additional Guidance (Page 18)	DG-5044 language: (OUO-SRI) Licensees should conduct random patrols, by trained staff, of CDAs that affect SSEP functions to look for obvious signs of cyber related tampering. NEI comment: Verify that random patrols are conducted by "trained" staff. Who does the training? How often. If supervisor raining [sic] lapses does this impact the ability if the patrol to continue patrols of CDAs?	The NRC's response to Comment Number 52 made this comment moot. Accordingly, the NRC has made no change to DG-5044 based on this comment. The NRC staff removed the "(OUO-SRI)" portion marking from this section, consistent with the Commission direction in the Staff Requirements Memorandum (SRM)—SECY-17-0095—Review and Approval of Proposed Revision to RG 5.77, "Insider Mitigation Program," dated July 14, 2021 (ML21195A356).
55. NEI	C.3.4.1, 1st Sentence (Page 18)	DG-5044 language: Licensees should have procedures available for operator response to events involving deliberate acts directed against plant equipment.	The NRC disagrees with the comment. The NRC specifically used the word operator in this sentence to address plant control room and external plant operators. Operators play a critical role in ensuring the safe and secure operation and if necessary,

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		NEI comment: Suggest a change in wording. Change “operator” to “operational” for clarity.	shutdown of a plant. Given their roles, it is important for operators to have clear procedures for addressing deliberate acts that could compromise plant equipment necessary for the safe operation or shut down of a plant. Accordingly, the NRC has made no change to DG-5044 based on this comment.
56. NEI	C.3.4.2 f (Page 19)	DG-5044 language: (OUO-SRI) Conduct random armed patrols of target set equipment or elements as required in 73.55(i)(5)(vi) NEI comment: Concern: 10 CFR 73.55(i)(5)(vi) does not require armed patrols of target sets. Additionally, the element (f) does not need to be marked OUO-SRI, as it restates a regulatory requirement. Recommendation: Item (f) should be revised to align with the requirement, as proposed in the suggested wording. The commenter proposed the following edit: “Conduct random ~~armed~~ patrols of target set equipment or elements as required in 73.55(i)(5)(vi).	The NRC agrees with the comment and has revised DG-5044 accordingly. The NRC staff removed the “(OUO-SRI)” portion marking from this section, consistent with the Commission direction in the Staff Requirements Memorandum (SRM)—SECY-17-0095—Review and Approval of Proposed Revision to RG 5.77, “Insider Mitigation Program,” dated July 14, 2021 (ML21195A356).
57. NEI	C.3.4.3 d (Page 20)	DG-5044 language: (OUO-SRI) While the above physical protection measures relate to target set equipment or elements, licensees should remain aware that tampering with non-target set equipment or	The NRC disagrees with the comment. The phrase “should remain aware” is used to remind licensees that tampering with non-target set equipment can also have an adverse impact on plant safety and security functions. Such impacts may affect a

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		support systems, such as safety, security, important to safety or emergency preparedness equipment, can adversely affect the ability to respond to events and comply with established regulations. NEI comment: The text "should remain aware" is difficult to define and quantify. The industry requests for definition [sic] by the NRC staff on the intent. In addition, what limits are the licensee to place on this requirement since there is a significant amount of such equipment outside of the PA.	licensee's ability to comply with existing regulations or to respond to unexpected events. The NRC has determined that the meaning of the phrase "should remain aware" does not need further explanation. Accordingly, the NRC has made no change to DG-5044 based on this comment. The NRC staff removed the "(OUO-SRI)" portion marking from this section, consistent with the Commission direction in the Staff Requirements Memorandum (SRM)—SECY-17-0095—Review and Approval of Proposed Revision to RG 5.77, "Insider Mitigation Program," dated July 14, 2021 (ML21195A356). This discussion has been relocated to Section C.3.4.3 a of DG-5044.
58. NEI	C.3.4.3 e, 3rd Sentence (Page 20)	DG-5044 language: (OUO-SRI) Licensees should train operations personnel to be sensitive to abnormalities that could be the result of tampering and to respond to such indications in a timely manner. During routine tours, operations personnel should be sensitive to changes in configurations that might indicate possible tampering. Licensees should review, determine, and provide training to operations personnel for target sets and target set equipment that may be disabled locally without any recognition by control room personnel that the equipment had been disabled prior to operation. NEI comment:	The NRC disagrees with the comment. Operators frequently engage in patrols to verify that plant equipment is operating properly. This guidance recommends that licensees provide operations personnel with training to be aware that abnormalities in equipment operations may be an indication of tampering. This guidance further recommends including training on target set and target set equipment. This training may be beneficial for the implementation of a licensee's insider mitigation program. Accordingly, the NRC has made no change to DG-5044 based on this comment. The NRC staff removed the "(OUO-SRI)" portion marking from this section, consistent with the

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		There is no regulatory basis to provide training to operations personnel for target sets and target set equipment. Furthermore "equipment that may be disabled locally without any recognition by the control room personnel that the equipment had been disabled prior to operation" is covered under previous subsections a) and b) of 3.4.3. The commenter proposed the following edit: "…During routine tours, operations personnel should be sensitive to changes in configurations that might indicate possible tampering. ~~Licensees should review, determine, and provide training to operations personnel for target sets and target set equipment that may be disabled locally without any recognition by control room personnel that the equipment had been disabled prior to operation."~~	Commission direction in the Staff Requirements Memorandum (SRM)—SECY-17-0095—Review and Approval of Proposed Revision to RG 5.77, "Insider Mitigation Program," dated July 14, 2021 (ML21195A356). This discussion has been relocated to Section C.3.4.3 b of DG-5044.
59. NEI	C.3.4.3 f, 1st Sentence (Page 20)	DG-5044 language: (OUO-SRI) As described in 10 CFR 73.55(i)(5)(vii), licensees shall train security personnel to recognize and respond to obvious indications of tampering. In accordance with 10 CFR 73.55(i)(5)(vi), licensees are required to provide random patrols of all accessible areas containing target set equipment. These patrols should be conducted by an armed security officer and should include all targets set equipment or elements, except where precluded by immediate personnel safety concerns, operational abnormalities, or restrictions, consistent with guidelines to keep radiation dose rates as low as reasonably achievable.	The NRC disagrees with the comment. The text is consistent with the 10 CFR 73.55(i)(5)(vii) requirement. Accordingly, the NRC has made no change to DG-5044 based on this comment. The NRC staff removed the "(OUO-SRI)" portion marking from this section, consistent with the Commission direction in the Staff Requirements Memorandum (SRM)—SECY-17-0095—Review and Approval of Proposed Revision to RG 5.77, "Insider Mitigation Program," dated July 14, 2021 (ML21195A356).

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		NEI comment: The commenter proposed the following edit: "(OUO-SRI) … ~~As described in 10 CFR 73.55(i)(5)(vii), licensees shall train security personnel to recognize and respond to obvious indications of tampering.~~ In accordance with 10 CFR 73.55(i)(5)(vi), licensees are required to provide random patrols of all accessible areas containing target set equipment…"	Based on administrative renumbering, this discussion now appears under Section 3.4.3 c of DG-5044.
60. NEI	C.3.4.3 h, 3rd Sentence (Page 20)	DG-5044 language: (OUO-SRI) Licensees should implement an armed patrol program applying special consideration to target set equipment. These patrols should also periodically assess the integrity of the barriers protecting and controlling access to target set equipment. NEI 03-12, describes the specifics of a patrol program that the NRC has found acceptable. NEI comment: The title of NEI 03-12 should be added for proper designation and clarification.	The NRC agrees with the intent of the comment but has not accepted the specific revision suggested by the commenter. Instead, the NRC has replaced the reference to "NEI 03-12" with a reference to "RG 5.76." The complete reference to RG 5.76 is included in the References section of DG-5044. The NRC staff also removed the "(OUO-SRI)" portion marking from this section, consistent with the Commission direction in the Staff Requirements Memorandum (SRM)—SECY-17-0095—Review and Approval of Proposed Revision to RG 5.77, "Insider Mitigation Program," dated July 14, 2021 (ML21195A356). Based on administrative renumbering, this discussion now appears under Section 3.4.3 e.
61. NEI	C.3.4.3 i, 3rd Sentence (Page 20)	NEI comment: The reference to NUREG/CR7145 should be added to the References.	The NRC agrees with the comment and has added NUREG/CR7145 to the References section of DG-5044.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
62. NEI	C.3.4.3 i, 4th Sentence (Page 20)	DG-5044 language: (OUO-SRI) … Armed patrols and surveillance mechanisms should provide for notification to at least two members of the response force. NEI comment: It is suggested that this sentence be deleted else a regulatory basis be provided. Delete or provide clarity and basis for statement.	The NRC disagrees with the comment. There is a requirement in 10 CFR 73.55(i)(2) that intrusion detection and video assessment equipment (surveillance mechanisms) must annunciate in two continuously staffed alarm stations. The sentence recommends, but does not require, that armed patrols also provide notifications to two members of the response force, which could include staff in one or both of the continuously staffed alarm stations. Accordingly, the NRC has made no change to DG-5044 based on this comment. The NRC staff removed the "(OUO-SRI)" portion marking from this section, consistent with the Commission direction in the Staff Requirements Memorandum (SRM)—SECY-17-0095—Review and Approval of Proposed Revision to RG 5.77, "Insider Mitigation Program," dated July 14, 2021 (ML21195A356). This discussion has been relocated to Section C.3.4.3 e.
63. NEI	C.4.1 (Page 21)	DG-5044 language: (OUO-SRI) A comprehensive and effective BOP will include a training program for recognizing and reporting behaviors as required in § 73.56(f)(3), which may be considered adverse to the safe operation and security of the licensee facility. NEI comment: 10 CFR 26.33, Behavior Observation has requirements that are pertinent to the IMP and probably should be referenced accordingly.	The NRC agrees with the comment and has added the reference to "10 CFR 26.33" to Section C.4.1 of the revised DG-5044. The NRC staff also removed the "(OUO-SRI)" portion marking from this section, consistent with the Commission direction in the Staff Requirements Memorandum (SRM)—SECY-17-0095—Review and Approval of Proposed Revision to RG 5.77, "Insider Mitigation Program," dated July 14, 2021 (ML21195A356).

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		The commenter proposed the following edit: "(OUO-SRI) A comprehensive and effective BOP will include a training program for recognizing and reporting behaviors as required in § 73.56(f)(3) and § 26.33, which may be considered adverse to the safe operation and security of the licensee facility.	
64. NEI	C.4.2 (Pages 21-22)	DG-5044 language: (OUO-SRI) Licensees should ensure that the BOP training includes recognition of and response to the following conditions or behavioral characteristics:… NEI comment: The paragraph includes 19 bullets representing specific training objectives. The bulleted items were added to the NEI 03-04, *Guideline for Plant Access and other Standardized Shared Training Courses and Evaluations* in December 2012. The industry believes that objectives, which were adapted from the Department of Homeland Security Suspicious Activity Reporting program further bolsters the awareness responsibilities of individuals subject to the industry's behavior observation program. Since the NEI 03-04 document is not endorsed by the NRC, the industry feels that its ability to immediately adapt to changing conditions in the observed in community or worldwide for that matter are a significant strength in the program. The rigid structure defined in the draft 5044 document lesson that ability to immediately respond to changes. The industry would prefer IMP text to	The NRC disagrees with the comment. The addition of the proposed wording "any other behavior inimical to facility safety or security" is overly vague and therefore overly broad. The NRC has determined that the proposed language is not necessary because the examples provided in Section C.4.2 adequately encompass the range of inimical behaviors that could adversely impact facility safety or security. Accordingly, the NRC has made no change to DG-5044 based on this comment. The NRC staff removed the "(OUO-SRI)" portion marking from this section, consistent with the Commission direction in the Staff Requirements Memorandum (SRM)—SECY-17-0095—Review and Approval of Proposed Revision to RG 5.77, "Insider Mitigation Program," dated July 14, 2021 (ML21195A356).

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		generically address conditions thus permitting the licensee to be flexible in addressing changing conditions. The commenter proposed adding a 20th bullet to end of the list of bulleted items in Section 4.2: "(OUO-SRI) any other behavior inimical to facility safety and security."	
65. NEI	C.5. FFD Program Elements During Decommission-ing (Pages 23-25)	NEI comment: The industry believes that decommissioning activities should be contained within a separate decommissioning document. The commenter proposed to the delete section "5. FFD Program Elements During Decommissioning."	The NRC disagrees with the commenter and has maintained Section C.5, "FFD Program Elements During Decommissioning" in DG-5044. The NRC response to Comment Number 3 discusses the ongoing decommissioning rulemaking, which is proposing revisions to 10 CFR Part 26 and the insider mitigation program.
66. NEI	Glossary, "Behavior Observation Program (BOP)" (Page 28)	DG-5044 language: An awareness program that meets requirements of both the access authorization and FFD programs. Personnel are trained to report legal actions; to possess certain knowledge and abilities related to abuse of drugs and alcohol and the recognition of behaviors adverse to the safe operation and security of the facility by observing the behavior of others in the workplace and detecting and reporting aberrant behavior or changes in behavior that might adversely impact an individual's trustworthiness or reliability; and undergo an annual supervisory review. NEI comment: The industry suggests the deletion of the word "awareness" to make the definition the same as in	The NRC disagrees with the comment. The behavioral observation program requires that licensee personnel should strive to be aware of and recognize behaviors adverse to the safe operation and security of the facility. Appropriate training is provided to licensee personnel to facilitate their awareness of such behaviors in the workplace, including detecting and reporting aberrant behavior or changes in behavior that might adversely impact an individual's trustworthiness or reliability. Accordingly, the NRC has made no change to DG-5044 based on this comment.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		RG 5.66 Attachment, NEI 03-01, Nuclear Power Plant Access Authorization Program. The definitions contained within NEI 03-01 are promulgated through industry documents (e.g., Policies, procedures, forms, etc.). Changing wording however, minor opens the inconsistency window during audits and inspections. Or leads to significant costs to change documents for no real improvement value. The commenter proposed the following edit: "An ~~awareness~~ program that meets requirements of both the access authorization and FFD programs…."	
67. NEI	Glossary, "Critical Group" (Page 28)	DG-5044 language: (OUO-SRI) … Any individual who performs job functions critical to the safe and secure operation of the licensee's facility. This individual includes any individual who has been granted UA or certified UAA and performs one or more of the following job functions: a. (OUO-SRI) any individuals who have extensive knowledge of facility defensive strategies or who design or implement the plant's defense strategies; b. (OUO-SRI) any individuals in a position to grant an individual unescorted access or to certify an individual unescorted access authorization; c. (OUO-SRI) any individuals assigned a duty to search for contraband (e.g., weapons, explosives, incendiary devices);	The NRC agrees with the comment, and has amended DG 5044, with minor modification. The additional text provided by the commenter is contained in the "Critical Group" description in Section C.2.1 of DG-5044. Moreover, the NRC has revised the "Critical Group" definition in the Glossary of DG-5044 to include the acceptable language in SFAQ 10-05, "IT functions for Critical Group," for consistency purposes. The NRC staff removed the "(OUO-SRI)" portion marking from this section, consistent with the Commission direction in the Staff Requirements Memorandum (SRM)—SECY-17-0095—Review and Approval of Proposed Revision to RG 5.77, "Insider Mitigation Program," dated July 14, 2021 (ML21195A356).

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		d. (OUO-SRI) any individuals who have access, extensive knowledge, or administrative control over plant digital computer and communication systems and networks as identified in 10 CFR 73.54. NEI comment: Revise definition to include the SFAQ 10-05 clarification and consistency with RG 5.66, Reference 4, NEI 03-01.	
68. NEI	Glossary, "Fitness for Duty Authorization (FFDA)" (Page 29)	DG-5044 language: A term commensurate with "authorization" as defined in 10 CFR 26.5, "Definitions." An element of UAA that identifies the status of an individual's required FFD elements, which are then evaluated by a reviewing official to determine whether the individual is trustworthy, reliable, and fit for duty. NEI comment: The industry suggests the inclusion [sic] the red text …to complete the definition of FFD Authorization and to be consistent with the text of NEI 03-01. The definitions contained within NEI 03-01 are promulgated through industry documents (e.g., policies procedures, forms, etc.) Changing wording however, minor opens the inconsistency window during audits and inspections. Or leads to significant costs to change documents for no real improvement value. The commenter proposed the following edits: "Fitness-for-Duty (FFD) Authorization (FFDA)—A term commensurate with "Authorization" as defined in 10 CFR 26.5. An element of UAA that	The NRC agrees with the comment and has revised the definition, with minor modification. In addition, the NRC deleted the first sentence of the definition: "A term commensurate with "authorization" as defined in 10 CFR 26.5, "Definitions."" The revised definition of "fitness for duty (FFD) authorization" states: "An element of unescorted access that identifies the status of an individual's required FFD elements, which are then evaluated by a reviewing official to determine the individual's trustworthiness, reliability, and FFD. These required elements for FFD authorization are consent, suitable inquiry (including education in lieu of employment and military service as employment), self-disclosure, pre-access drug and alcohol testing, and being subject to both a licensee approved behavioral observation and random drug and alcohol testing program."

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		identifies the status of an individual's required fitness-for-duty elements, which are then evaluated by a reviewing official to determine whether the individual is trustworthy, reliable and fit for duty. The required elements for FFDA are: consent, suitable inquiry (including education in lieu of employment and military service as employment); self- disclosure; pre-access drug and alcohol testing; training in the required FFD K&A's, FFD and BOP); being subject to both licensee-approved BOP and drug and a alcohol testing program."	
69. NEI	Glossary, "Insider" (Page 29)	DG-5044 language: A person who has been granted unescorted access or unescorted access authorization under the requirements of 10 CFR 73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants," or has the ability to access information systems that: (1) connect to systems that connect to plant operating systems, or (2) contain sensitive information that may assist in an attempted act of sabotage. NEI comment: The industry suggests the inclusion the red text in the next column to complete the definition of Insider and to be consistent with the text of NEI 03-01. The definitions contained within NEI 03-01 are promulgated through industry documents (e.g., policies procedures, forms, etc.) Changing wording however, minor opens the inconsistency window during audits and inspections. Or leads to significant costs to change documents for no real improvement value.	The NRC disagrees with the comment. Definitions should remain as consistent as possible within regulatory guidance documents authored by the NRC. The NRC defines "insider" within the Glossary of Security Terms for Nuclear Power Reactors NUREG-2203 dated February 2017 and RG 5.69, "Guidance for the Application of the Radiological Sabotage Design-Basis Threat in the Design, Development, and Implementation of a Physical Security Program that meets 10 CFR 73.55 Requirements," (SGI), providing consistency within DG-5044 glossary section. NEI 03-01, while endorsed by the NRC staff, is not a document authored by the NRC. Accordingly, the NRC has made no change to DG-5044 based on this comment.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		The commenter proposed the following edits: "…or (2) contain sensitive information that could benefit an insider."	
70. NEI	Glossary, "Reviewing Official" (Page 29)	DG-5044 language: The licensee or, if applicable, the contractor or vendor, persons designated by their company to be responsible for reviewing and evaluating all data collected about an individual, including potentially disqualifying information, in order to determine whether the individual may be authorized UAA or granted UA. NEI comment: The definition is not consistent with RG 5.66, Reference 4. The certification of UAA and/or the granting of UA is a licensee responsibility. The commenter proposed the following edit: "...including potentially disqualifying information, in order to determine whether the individual may be certified UAA by a licensee or C/V, or granted UA by a licensee."	The NRC agrees with the comment and has revised the definition, with minor modification. The revised definition of "reviewing officials" states: "Persons designated by the licensee or, if applicable, the contractor or vendor, to be responsible for reviewing and evaluating data collected about an individual, including potentially disqualifying information, to determine whether the individual may be certified for unescorted access authorization or granted unescorted access by a licensee."
71. NEI	C.1, (about Page 4)	DG-5044 language: …implementation of measures that control personnel access to the licensee's … NEI comment: Safety-related systems are not listed (they may not necessarily be part of the target set elements), yet the computer networks associated with safety-related and important to safety are listed.	The NRC disagrees with the comment. As stated, in part, in 10 CFR 73.54(a)(1), the licensee is required to protect digital computer and communication systems and networks associated with "safety-related and important-to-safety functions." However, the wording of this discussion has been revised to be consistent with language of the regulation. Accordingly, the NRC has made no change to DG-5044 based on this comment.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
		Change vi to read, "…computer networks associated with target sets, security functions and emergency preparedness functions…"	
72. NEI	B. Discussion, Harmonization with International Standards, (Page 6)	NEI comment: This regulatory guide revision doesn't include visitor information contained in IAEA Nuclear Security Series No. 8. The regulatory guide lacks any mention of concern with visitors. "Escort and surveillance of infrequent workers and visitors. Temporary workers, such as maintenance, service or construction workers, often come from contracting or subcontracting companies. The trustworthiness of temporary workers and visitors may not have been determined prior to their being permitted access. Escorting such people is a way of making sure that they are in the right place and that they are performing their duties properly. To be effective, the escort should know about their approved activities, including access to specific places and actions they should not perform. In addition, guard patrols may deter or detect any attempt by individuals to carry out malicious acts."	The NRC disagrees with the comment. The requirements for visitors are captured in 10 CFR 73.55(g)(7). The International Atomic Energy Agency (IAEA) Nuclear Security Series No. 8 contains similar guidelines and is cited as reference No.13 within DG-5044. The NRC has revised the section title "Harmonization with International Standards to read "Consideration of International Standards." This section also has been revised to state: "The International Atomic Energy Agency (IAEA) works with member states and other partners to promote the safe, secure, and peaceful use of nuclear technologies. The IAEA develops safety requirements and safety guides for protecting people and the environment from harmful effects of ionizing radiation. This system of safety fundamentals, safety requirements, safety guides, and other relevant reports, reflects an international perspective on what constitutes a high level of safety. To inform its development of this RG, the NRC considered IAEA safety requirements and safety guides pursuant to the Commission's International Policy Statement (Ref. 11) and Management Directive and Handbook 6.6, "Regulatory Guides," dated May 2, 2016 (Ref. 12).

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
			The staff considered the following IAEA safety requirements and guide in the development and update of the RG: IAEA Nuclear Security Series No. 8-G, "Preventive and Protective Measures against Insider Threats," Revision 1, issued 2020 (Ref. 13)."
73. NEI	C.1. General Requirements, (Page 8)	NEI comment: Licensee or applicant's RO….determine what access level for the individual	It is not clear what change this comment is recommending. The NRC has determined that the current language addressing the responsibilities of the licensee's or applicant's Reviewing Official is appropriate. Accordingly, the NRC has made no change to DG-5044 based on this comment.
74. NEI	C.2. Applicability, 1st paragraph	NEI comment: Requires an initial and periodic medical assessment, to include a psychological evaluations… Should be, "Requires a psychological evaluation, which may include a medical assessment…"	The NRC disagrees with the comment. The language is consistent with the language contained in DBT Order, EA-03-086, Attachment 2, page 5. Accordingly, the NRC has made no change to DG-5044 based on this comment.
75. NEI	C.1.2, 1st Paragraph, (Page 9)"	NEI comment: No mention of escorted workers, e.g., visitors Add "escorted workers" or "visitors".	The NRC disagrees with the comment. The language in the section referenced by the comment is a high-level discussion of the motivations and unpredictable nature of an insider and the insider threat. The reference to a disgruntled employee is only an example of one type of insider threat. This discussion is not meant to address all types of insider threats that a licensee might face. The NRC further notes that the requirements for visitors are captured in 10 CFR 73.55(g)(7). Accordingly, the NRC has made no change to DG-5044 based on this comment.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
76. NEI	C.2. Applicability	NEI comment: DBT Order, EA–03–086 -- It's listed several times. What portions of this order are still valid?	The NRC notes that NRC Order EA-03-086 was issued on February 25, 2002, and was revised on April 29, 2003. All elements in the revised order remain in effect and have not been rescinded or modified.
77. NEI	Glossary	NEI comment: Add FFD staff and reword to reflect current critical group definition as in SFAQ 10-05.	The NRC disagrees with the comment. SFAQ 10-05 does not make any reference to FFD staff as part of the critical group. Personnel addressing FFD issues are governed by the requirements of 10 CFR Part 26. While the NRC acknowledges that FFD elements play a role in the IMP, to the extent that a definition of FFD staff is needed it should properly be in 10 CFR Part 26 or the 10 CFR Part 26 associated guidance. Accordingly, the NRC has made no change to DG-5044 based on this comment.
78. NEI	Glossary	NEI comment: Add escorted worker definition.	The NRC disagrees with the comment. Escorted workers fall under the category of "visitors." The requirements for visitors are captured in 10 CFR 73.55(g)(7). Accordingly, the NRC has made no change to DG-5044 based on this comment.
79. NEI	References	NEI comment: References section doesn't include all references in the document (e.g., IEA nuclear security series #8, SAND2007-5591, NUREG/CR-7145).	The NRC agrees with the comment. The identified references have been added to the References section of the revised DG-5044.
80. NEI	References	NEI comment: NUREG-1959 hasn't been listed before and reads like we're now required to use it. Change to "provides a detailed discussion of proximity sensors, which may be used as part of an IMP."	The NRC agrees with the comment. The discussion of NUREG 1959 in the related Guidance section of the revised DG-5044 makes clear that proximity sensors may be used.

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
81. NEI	C.3.5.3	NEI comment: Deleted the reference to NEI 03-12 and statement that the guidance in NEI 03-12 provides the specifics of a patrol program that the NRC has found acceptable. Why was this reference deleted? Doesn't this leave licensees open to subjective judgments regarding what a satisfactory patrol program consists of that is outside the guidance of NEI 03-12 regarding frequency, locations, depth of patrols, etc.?	The NRC agrees with the comment. However, the NRC believes that the commenter may have inadvertently referred incorrectly to Section 3.5.3 of DG-5044. DG-5044 contains no Section 3.5.3 within the document. The correct reference is Section 3.4.3. Guidance on an acceptable security patrol program can be found under Regulatory Guide 5.76, "Physical Protection Programs at Nuclear Power Reactors" (SGI). The reference to NEI 03-12 has been removed from DG-5044 because it is redundant to the guidance found in RG. 5.76.
82. UCS	1 (vi)	UCS comment: The IMP should not overlook insider access to systems that may not have a direct nexus to SSEP but may provide information useful to an adversary – eg. Personal information on staff that could be used for blackmail.	The NRC agrees with this comment. Consistent with 10 CFR 73.55(b)(9)(iii), the foundation of the insider mitigation program is to ensure that licensees implement defense-in-depth methodologies to minimize the potential for an insider to adversely affect a licensee's capability to prevent significant core damage and spent fuel sabotage. The comment does not make any specific recommendation for a revision to DG-5044. Accordingly, the NRC has made no change to DG-5044 based on this comment.
83. UCS	C.4 Behavior Observation Training	UCS comment: NRC should not limit the scope of this section as proposed by NEI. (BOP)	The NRC agrees with the comment. Section 4 of DG-5044 discusses the Behavioral Observation Program (BOP). This section provides a high-level discussion consistent with the applicable requirements in 10 CFR 73.56(f). The NRC has not accepted recommendations to limit the scope of the BOP that are inconsistent with these requirements. The comment does not make any specific recommendation for a revision to

Comment	DG-5044 Section	Specific Comments	NRC Comment Resolution
			DG-5044. Accordingly, the NRC has made no change to DG-5044 based on this comment.
84. UCS	Not applicable	UCS comment: General Comment. It should be evident today that the insider threat is posing an ever-growing risk to sensitive information and facilities. The NRC must be vigilant in ensuring that licensees maintain robust and broad programs to protect against insiders. A growing danger today is the insider who has received sophisticated training on how to evade being detected by conventional insider mitigation programs. Therefore, such programs themselves must evolve in order to detect such training.	The NRC agrees with the comment. The NRC continuously monitors the current threat environment for any changes that may impact NRC licensed facilities, materials, and/or other activities. The NRC currently has no indication of any impact or change to the threat environment for our licensed facilities, materials, and activities. The NRC continues to coordinate with our Federal partners to ensure we are providing prompt assessment of any security threats to our licensed facilities, materials, and activities. Should any change to the threat landscape emerge, NRC will take prompt and appropriate action to address any security threats to our licensed facilities, materials, and activities. The comment does not make any specific recommendation for a revision to DG-5044. Accordingly, the NRC has made no change to DG-5044 based on this comment.
85. UCS	C.2.2, The Critical Group, 2nd Paragraph, Items (1) to (5)	UCS comment: Why was this deleted? Where did it go?	The NRC notes that the elements of the critical group were not deleted from DG-5044. The NRC relocated this information to the Glossary of revised DG-5044 in the definition of “information technology (IT) personnel.”