Audit of the U.S. Nuclear Regulatory Commission's Cybersecurity Inspection Program for Operating Nuclear Power Plants

OIG-NRC-26-A-03

June 4, 2026

All publicly available OIG reports
are accessible through the OIG's website at:
nrcoig.oversight.gov

MEMORANDUM

DATE: June 4, 2026

TO: Michael F. King
Executive Director for Operations

FROM: Hruta Virkar, CPA */RA/*
Assistant Inspector General for Audits & Evaluations

SUBJECT: AUDIT OF THE U.S. NUCLEAR REGULATORY COMMISSION'S CYBERSECURITY INSPECTION PROGRAM FOR OPERATING NUCLEAR POWER PLANTS (OIG-NRC-26-A-03)

Attached is the Office of the Inspector General's (OIG) audit report titled: *Audit of the U.S. Nuclear Regulatory Commission's Cybersecurity Inspection Program for Operating Nuclear Power Plants.*

The report presents the results of the subject audit. Agency staff indicated that they had no formal comments for inclusion in this report and waived the exit conference.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this memorandum.

We appreciate the cooperation extended to us by members of your staff during the audit. If you have any questions or comments about our report, please contact me at 301.415.1982 or Mike Blair, Team Leader, at 301.415.8399.

Attachment:
As stated

cc: D. Curtis, ADO
S. Anderson, Acting DADO
E. Deeds, OEDO

Results in Brief

Audit of the U.S. Nuclear Regulatory Commission's Cybersecurity Inspection Program for Operating Nuclear Power Plants

OIG-NRC-26-A-03
June 4, 2026

Why We Did This Review

Title 10 of the *Code of Federal Regulations* (10 C.F.R.) section 73.54 requires each nuclear power plant to provide high assurance that its digital computer and communication systems and networks are adequately protected against cyber attacks.

NRC staff and contractors use Inspection Procedure (IP) 71130.10, "Cybersecurity," and supporting inspection guidance to inspect licensees' cybersecurity programs and verify licensee compliance with 10 C.F.R. section 73.54. Since 2022, the NRC has completed two cycles of baseline cybersecurity inspections, identifying hundreds of performance deficiencies across operating nuclear power plants. These findings underscore the importance of continued oversight and program improvement.

The audit objective was to determine if the NRC's cybersecurity inspection program for operating nuclear plants is robust and adaptive to evolving cyber threats.

What We Found

The OIG determined that the U.S. Nuclear Regulatory Commission's (NRC) cybersecurity inspection program for operating nuclear plants is fundamentally robust and adaptive to emerging cyber threats. However, addressing operational inefficiencies is essential to maximize the program's effectiveness.

Specifically, the OIG determined:

- The current cybersecurity program guidance lacks clarity;
- Expectations for maintaining training qualifications are not well-defined;
- The cybersecurity inspection process contains redundant and time-consuming tasks; and,
- NRC staff members did not always accurately report their time spent on cybersecurity inspection-related activities.

What We Recommend

This report makes 9 recommendations to enhance the effectiveness, consistency, and efficiency of the NRC's cybersecurity inspection program.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

10 C.F.R.	Title 10 of the *Code of Federal Regulations*
CAC	Cost Activity Code
CSP	Cybersecurity Plan
EDO	Executive Director for Operations
EPID	Enterprise Project Identifier
HCM	Human Capital Management
IMC	Inspection Manual Chapter
IP	Inspection Procedure
NEI	Nuclear Energy Institute
NRC	U.S. Nuclear Regulatory Commission
NSIR	Office of Nuclear Security and Incident Response
OIG	Office of the Inspector General
RFI	Request for Information
RG	Regulatory Guide
SIF	Security Issues Forum

I. BACKGROUND

As of January 2026, there are 55 operating NRC-licensed nuclear power plants in the United States, housing a total of 94 reactors.[1] These nuclear power facilities rely on digital systems to monitor, operate, control, and protect plant operations. To safeguard critical digital assets that support safety and security functions, these systems are isolated from external networks, including the internet. Nevertheless, all power reactor licensees are required to implement a cybersecurity plan (CSP) in accordance with 10 C.F.R. section 73.54. Issued in 2009, this regulation mandates that NRC-licensed nuclear power plants protect digital systems and components associated with safety, security, and emergency preparedness functions from cyber attacks.

Under section 73.54, licensees are required to develop and maintain NRC-approved CSPs detailing the measures, procedures, and documentation necessary to meet the NRC's requirements for protecting digital computer and communication systems and networks associated with specified functions. These site-specific CSPs are typically developed using guidance provided in either the NRC's Regulatory Guide (RG) 5.71, Revision 1, *Cybersecurity Programs for Nuclear Power Reactors,* or the NRC-endorsed Nuclear Energy Institute (NEI) 08-09, Revision 6, *Cyber Security Plan for Nuclear Power Reactors*.[2] Both documents outline approaches for complying with cybersecurity regulations and identify 147 technical, operational, and management security controls that licensees must implement at their facilities. Of the 55 operating NRC-licensed nuclear power plants, only one developed its cybersecurity plan using RG 5.71; the remaining 54 used the NEI 08-09, Rev. 6 template.

The NRC developed its cybersecurity inspection program to verify regulatory compliance and ensure that operating power reactor licensees implement cybersecurity programs at their facilities as described in their NRC-accepted CSPs.

[1] Three nuclear power plants are in RESTART status and are expected to be in operating status soon. RESTART refers to the process when a plant applies to transition from a decommissioned reactor to resume operations as an active reactor.

[2] NEI is an independent organization that represents the nuclear energy industry in policy matters. At NEI's request, the NRC reviewed NEI 08-09, Rev. 6 (April 2010) and determined its cybersecurity plan template provides an acceptable approach for licensees to comply with federal requirements under 10 C.F.R. section 73.54.

In 2022, the NRC incorporated cybersecurity inspections into the agency's Reactor Oversight Process baseline inspections.[3] From 2022 to 2025, cybersecurity baseline inspections were conducted every two years; however, beginning in 2026, the inspection frequency will change to every three years. To date, the NRC has completed two full inspection cycles and has initiated its third.

Cybersecurity Inspection Program Management

Various NRC offices and staff are responsible for maintaining and implementing the cybersecurity inspection program.

Office of Nuclear Security and Incident Response

The Office of Nuclear Security and Incident Response (NSIR) develops the overall agency policy and provides management direction for the evaluation and assessment of technical security issues at nuclear facilities. NSIR established the Cyber Security Branch in 2013 to enhance internal governance of the NRC's cybersecurity regulatory activities. The Cyber Security Branch plans, coordinates, and manages the NRC's cybersecurity activities related to applicants and licensees. Its responsibilities encompass rulemaking, guidance development, licensing, policy formulation, and oversight of cybersecurity requirements. In addition, the Cyber Security Branch develops inspection guidance and establishes qualification and training requirements for cybersecurity inspectors. Cyber Security Branch staff may also participate in inspections to provide technical expertise and support.

To further strengthen its capabilities, the Cyber Security Branch receives contractor support. Under a 5-year labor-hour contract, the cybersecurity contractor employees assist with inspection activities, provide knowledge management training for the inspection program, and contribute technical expertise to the NRC's cybersecurity regulatory framework for all licensees, applicants, and certificate holders. This contract is set to expire on August 17, 2026. Another contract is expected to be in place at the conclusion of the current contract.

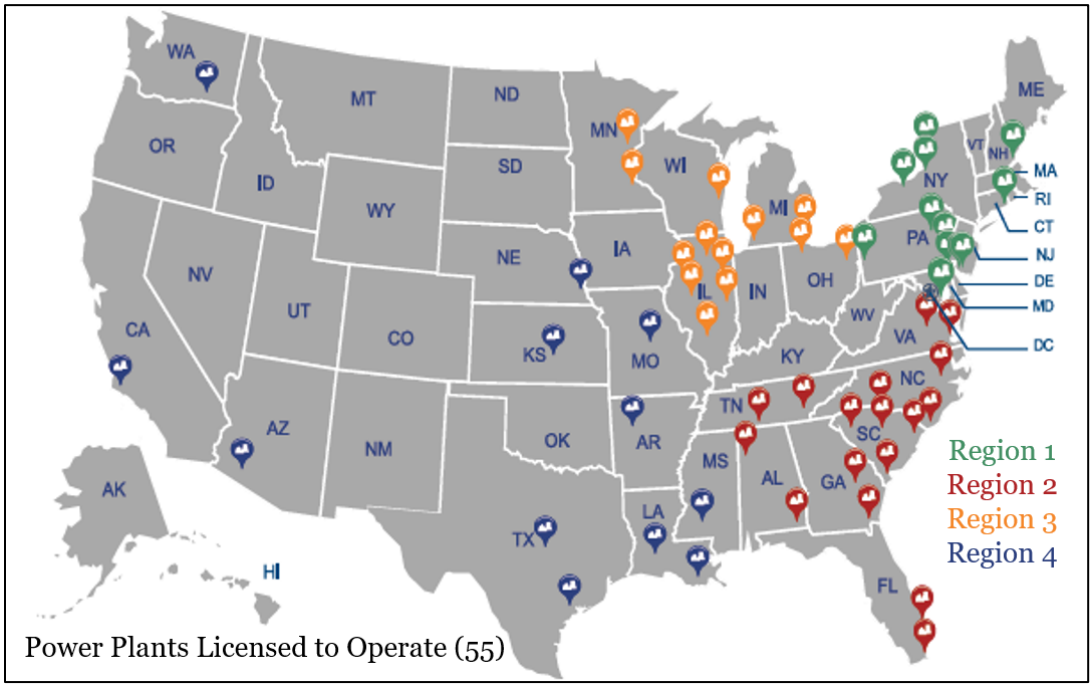
NRC's Regional Offices

Although NSIR oversees the cybersecurity program, each NRC regional reactor inspector is responsible for a broad range of inspections, including inspections

[3] The NRC's Reactor Oversight Process is the NRC's framework for inspecting and assessing licensee performance in a risk-informed, objective, predictable, and understandable way. It provides a means to collect information about licensee performance, assess the information for its safety significance, and provide for appropriate licensee and NRC responses.

relating to cybersecurity, electrical systems, digital instrumentation and control, and fire protection.[4] With assistance from NSIR's contractor employees, inspectors conduct inspections within their assigned regions using NRC-approved cybersecurity inspection guidance.[5] As needed, regional inspectors may support one another across regions to ensure comprehensive coverage and consistency in inspection practices. Figure 1 illustrates all operating reactors in the United States, color-coded by the NRC region responsible for inspections.

Figure 1: Operating Nuclear Power Plants in the United States as of March 2026



Source: NUREG-1350, Volume 35, "Information Digest"

Prior to 2026, each inspection team consisted of two NRC-qualified cybersecurity inspectors and two contractors. Beginning in 2026, two NRC-qualified cybersecurity inspectors and one contractor employee will conduct inspections.

[4] These inspectors come from Engineering Branch 2 of their respective regions.

[5] While contractors support the inspection team by providing expertise, NRC inspectors have full responsibility for leading and completing cybersecurity inspections. Contractors cannot represent or speak on behalf of the NRC; their role is to serve as cybersecurity subject matter experts within the inspection team.

Inspector Qualification and Proficiency Requirements

To perform any technical inspections, the NRC's inspectors are required to complete Inspection Manual Chapter (IMC) 1245, Appendix A, "Basic Level Training and Qualification Journal." Inspectors assigned to cybersecurity inspections require additional training qualifications in accordance with IMC 1245, Appendix C-14, "Cybersecurity Inspector Technical Proficiency Training and Qualification Journal." To maintain the cybersecurity inspector qualification, inspectors must complete at least one cybersecurity inspection every three years and attend the Annual Cybersecurity Counterpart Meeting coordinated by the Cyber Security Branch. This meeting provides a forum for Cyber Security Branch staff and regional inspectors to share updates on the cybersecurity inspection program, exchange insights, and address inspection challenges.

The NRC currently has 24 qualified cybersecurity inspectors, with an average of approximately three years of experience. While some inspectors possess more than six years of individual experience, eight inspectors have less than one year of experience.

Inspection Process and Guidance

The NRC's cybersecurity inspection process aims to provide reasonable assurance that the licensee's digital computer and communication systems and networks associated with safety, important-to-safety, security, and emergency preparedness functions are adequately protected against cyberattacks. These inspections follow a structured approach designed to evaluate the effectiveness of licensee cybersecurity programs.

Request for Information

The inspection process begins with a series of requests for information (RFIs), which help the inspection teams gather relevant program data, develop a site-specific inspection plan, and prepare for on-site activities. The NRC's *Guidance Document for Development of the Request for Information and Notification Letter for IP 71130.10 Cyber Security Inspection* describes the types of information typically requested, enabling inspectors to make informed decisions during the planning phase.

During the planning phase of each inspection, and prior to the on-site inspection, inspectors send three sequential RFIs to licensees. These RFIs request information

related to cybersecurity policies and procedures, security control assessments, network defensive architecture, and other matters. The cybersecurity inspection team uses the information collected to select systems for sampling and request more targeted data on those systems. More questions may arise during inspector walkdowns or meetings with the licensee while the cybersecurity inspection team is on site, in which case the questions would constitute a fourth RFI. Table 1 summarizes the communication timeline established in the cybersecurity RFI guidance.

Table 1: RFI Communications Expectations

RFI #	Information Requested	Due
RFI 1 issued	Generic information about licensee's programs	120 days prior to the on-site inspection
Licensee response due		12 weeks prior to on-site inspection
RFI 2 issued	Information specific to critical digital assets selected for sampling	8 weeks prior to on-site inspection
Licensee response due		4 weeks prior to on-site inspection
RFI 3 issued	Outstanding questions related to the sampled systems	Friday before on site
Licensee response due		First day on site
RFI 4	Questions that arise during inspections	Due while on site

Source: OIG created based on the RFI template

On-site Inspection

After the third RFI is issued, inspectors conduct the inspection in accordance with the requirements in Inspection Procedure (IP) 71130.10. IP 71130.10 establishes a standardized framework for NRC inspectors to evaluate nuclear facilities' cybersecurity programs. It defines objectives, inspection requirements, and guidance for assessing whether licensees adequately protect digital systems tied to safety, security, and emergency preparedness. This IP helps inspectors efficiently verify compliance with regulations like 10 C.F.R. section 73.54 and maintain consistent oversight. The IP covers key areas such as monitoring, defense-in-depth,

configuration management, program reviews, and corrective actions to ensure systems are safeguarded against cyberthreats and aligned with regulatory standards.

Under IP 711.30, the on-site inspection is expected to involve one week of direct inspection that takes two inspectors approximately 35 hours each (70 hours total) over five workdays to complete. In the first 3.5 days, the inspection team completes facility walkdowns, conducts interviews, and discusses issues of concern with the licensee. The inspection team then spends the remainder of the fourth day and the morning of the fifth day finalizing its findings. Once the inspection findings are complete, the team holds an exit meeting with the licensee on the fifth day to present the findings.

Cyber Security Issues Forum

Following the on-site cybersecurity inspection, the NRC convenes a Cyber Security Issues Forum (SIF) to facilitate discussion of findings and promote knowledge sharing among regional and headquarters staff. Based on these discussions, findings may be accepted or clarified, and the designated severity level of the findings may be changed or overturned by the inspecting region.

NSIR is responsible for organizing, scheduling, and facilitating the Cyber SIFs after each inspection. To ensure a comprehensive review and promote cross-regional collaboration, each Cyber SIF includes a required group of participants. These participants include staff from the Cyber Security Branch, the inspection team members and their branch chief, and a branch chief or designee from each of the other three NRC regions. While regional inspectors who were not directly involved in the inspection are encouraged to attend, their participation is not mandatory. Guidance for coordinating Cyber SIFs is provided in the cybersecurity issues forum charter. The Cyber Security Branch has also developed a dashboard to make scheduling Cyber SIFs more efficient and to consolidate all cybersecurity inspection findings for inspectors to use in monitoring trends and data.

Finally, the inspection report is issued within 45 days of inspection completion, which is typically the last day of the on-site inspection.

Changes to the Reactor Oversight Process

In May 2025, Executive Order 14300, *Ordering the Reform of the Nuclear Regulatory Commission*, directed the NRC to revise the Reactor Oversight Process to reduce unnecessary regulatory burdens and better address credible risks. In

response, the NRC is re-baselining[6] its inspection guidance, which includes IP 71130.10. The updated cybersecurity IP is intended to make inspections more efficient and effective with reduced inspection requirements. Other revisions include reducing the inspection team size and changing inspections from biennial to triennial, which would reduce the number of annual cybersecurity inspections from 27 to 19. Since July 1, 2025, cybersecurity inspections have been conducted at the minimum level necessary until all security baseline inspection procedures are re-baselined.

II. OBJECTIVE

The audit objective was to determine if the NRC's cybersecurity inspection program for operating nuclear plants is robust and adaptive to evolving cyber threats.

III. FINDINGS

The OIG defines a robust program as one that has a sound foundation for implementing the inspection program: qualified inspectors, efficient and effective inspection processes, and sufficient resources to carry them out. Since the inception of the cybersecurity program, the NRC has maintained a robust program by creating guidance that encompasses inspection planning, implementation, and closure; developing introductory and advanced cybersecurity training for inspectors seeking cybersecurity qualifications; and, promoting the cybersecurity inspector qualification to its inspectors to ensure inspector availability for inspections.

The OIG defines an adaptive program as a program that adjusts and evolves as the environment changes. The NRC's cybersecurity inspection program is adaptive to changing cyber threats because it incorporates lessons learned from cybersecurity inspections in its inspection practices, uses staff and contractor employees with relevant expertise to understand the most recent cyberthreats that may impact the cybersecurity inspection program, frequently engages with industry to stay abreast of potential challenges with maintaining cybersecurity programs in power reactors, and updates its advanced cybersecurity inspector training for up-and-coming inspectors.

Although the NRC's cybersecurity inspection program for operating nuclear plants is robust and adaptive to changing cyberthreats, the agency must address operational

[6] Re-baselining is the NRC's assessment of its work performed across the agency to determine which activities can be shed, de-prioritized, or performed with a less intense resource commitment.

inefficiencies to maximize the program's effectiveness. Specifically, the OIG determined:

1. The current cybersecurity program guidance lacks clarity;
2. Expectations for maintaining training qualifications are not well-defined;
3. The cybersecurity inspection process contains redundant and time-consuming tasks; and,
4. NRC staff members did not always accurately report their time spent on cybersecurity inspection-related activities.

1. The Current Cybersecurity Program Guidance Lacks Clarity

The NRC's Principles of Good Regulation require a clear nexus between the agency's regulatory guidance and its goals and objectives. In the context of the NRC's cybersecurity program, however, the guidance and its expected implementation by licensees and inspectors do not align. This disconnect is due to the lack of supplemental guidance for evaluating controls, which has resulted in misaligned expectations, inconsistent interpretations, and inefficiencies during inspections.

What Is Required

Regulatory Guidance should have a Clear Nexus to Regulatory Goals

Consistent with the NRC's Principles of Good Regulation, guidance should be coherent, logical, and practical. There should be a clear nexus between regulations and agency goals and objectives, whether explicitly or implicitly stated. Agency positions should be readily understood and easily applied. The U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government*[7] also state that management should define objectives in specific terms, so that they are understood at all levels of the organization. This involves clearly defining what is to be achieved, who is to achieve it, and how and when it will be achieved.

What We Found

A Disconnect Exists Between the Guidance and Its Expected Implementation, and how Findings are Determined

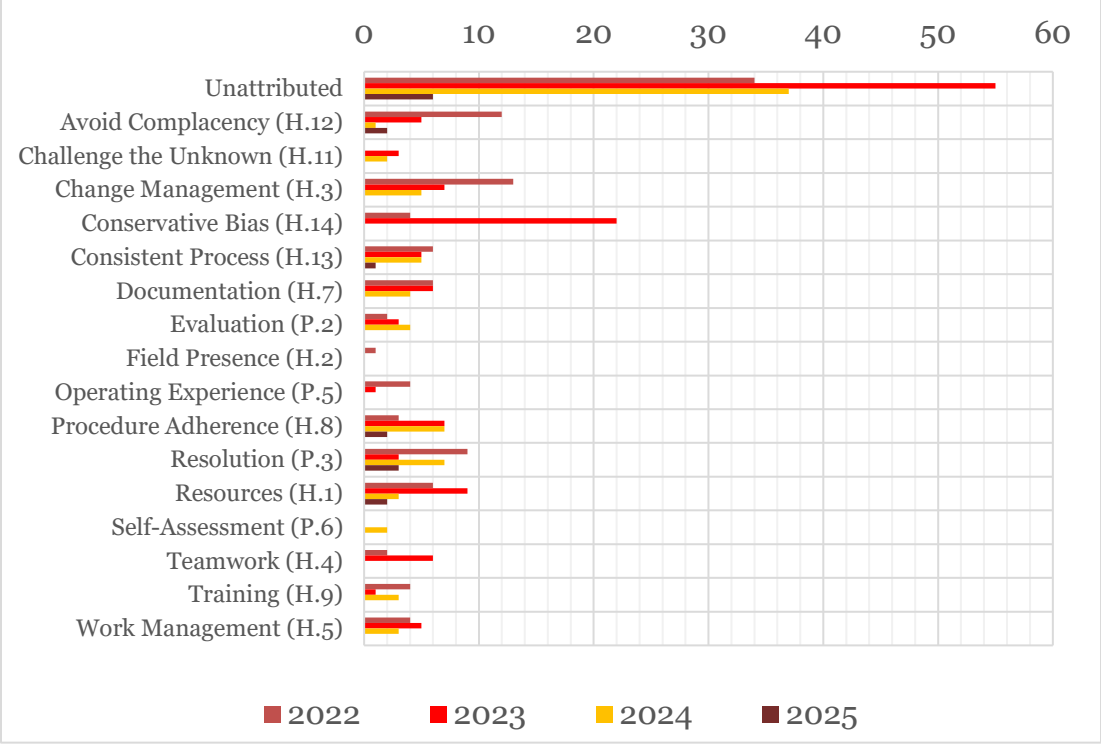
While RG 5.71 provides an acceptable framework for meeting the cybersecurity

[7] GAO-25-107721, May 2025

requirements of 10 C.F.R. section 73.54, and while NEI 08-09 offers an NRC-endorsed method for developing CSPs, these documents do not fully translate into consistent implementation and evaluation practices. Licensees use these documents to tailor their site-specific cybersecurity programs; however, a disconnect exists between how licensees apply and evaluate their programs and how NRC inspectors assess them.

Cybersecurity findings have accounted for the most NRC security findings since 2022, with inspectors identifying 339 performance deficiencies across 73 different NEI 08-09 cybersecurity controls (see Figure 2). Some licensees stated to the OIG that many findings have resulted from unclear guidance they receive for implementing and evaluating cybersecurity controls, as well as from inspectors evaluating those controls inconsistently based on their own interpretations of how licensees should implement them.

Figure 2: NRC-identified cross-cutting aspects for cybersecurity controls with performance deficiencies, January 2022 – September 2025



Source: OIG generated from Cybersecurity Inspection Findings

During the OIG's observation of an NRC inspection, the OIG observed multiple discussions between the licensee and the inspection team regarding how particular controls should be evaluated, indicating varied understandings or interpretations of

the agency's regulatory guidance. Inspectors evaluated the licensee's critical digital asset controls differently than the licensee expected, highlighting an inconsistency in interpretation.

Furthermore, IP 71130.10 includes a vague reference to Cyber SIFs. Licensees understand that findings may change based on discussions with NRC staff and inspectors; however, the procedure does not explain how Cyber SIFs might also influence those findings. Cyber SIFs are conducted after every cybersecurity inspection to ensure consistent evaluation of findings and violations, and these discussions can lead to changes in how a finding is characterized based on inspection experience at other sites.

Why This Occurred

Guidance for Evaluating Controls and Determining Findings is Unclear

RG 5.71 and NEI 08-09 are high-level documents that lack detail on the extent to which the specified cybersecurity controls should be implemented, and how the controls should be consistently evaluated. The NRC has not issued supplemental guidance to clarify these areas for either licensees or inspectors. As a result, licensees only find out how the agency intends to implement the guidance through discussions during inspections, forums, and conferences with the agency. However, those discussions are not recorded or documented. Additionally, inspectors noted they would like more examples of cybersecurity controls to understand how they were previously evaluated, but the NRC had not updated IMC 0612, Appendix E, "Examples of Minor Issues," since November 2023, which was before the first baseline inspection cycle was completed.

IP 71130.10 needs additional updates. Although it was recently revised, it still does not clearly distinguish between the physical security SIF, which is used at the staff's discretion to discuss physical security findings, and the Cyber SIF, which is required after every cybersecurity inspection.

Why This Is Important

Interpretation Gaps Lead to Inefficiencies

Overall, ineffective guidance leads to inconsistent cybersecurity program evaluations by licensees and inspectors. This inconsistency between evaluation requirements and NRC expectations may lead to inconsistent outcomes and result in preventable

deficiencies. Further, during the on-site inspection, inspectors may spend more time evaluating potential findings and discussing whether licensees are meeting applicable requirements, reducing the efficiency and consistency of the cybersecurity oversight process. Clear and logical supplemental guidance will help the NRC consistently implement the cybersecurity program and conduct inspection activities efficiently.

Additionally, when Cyber SIF discussions lead to changes in inspection determinations, licensees may not understand why findings were modified, reduced, or removed, especially since IP 71130.10 does not explain this process. Clarifying how internal discussions influence inspection outcomes would help address industry concerns about consistency in cybersecurity inspections. This need for clarity is even more important as the agency plans to eliminate IMC 0612, Appendix E, and revise the significance determination process, actions that may increase the frequency or depth of Cyber SIF discussions as inspectors apply updated screening criteria.

Recommendations

The OIG recommends that the Executive Director for Operations (EDO):

1.1. Develop and issue supplemental guidance clarifying the expected implementation of cybersecurity controls, the interpretation of requirements, and methods for evaluating control effectiveness; and,

1.2. Update Inspection Procedure 71130.10 to clarify the Cyber Security Issues Forum process and its potential impacts on findings and violations.

2. Expectations for Maintaining Training Qualifications are not Well-Defined

Expectations for training and training qualifications should be clearly defined. We found that expectations for completing refresher training and maintaining training qualifications for cybersecurity inspectors are not well-defined. This occurred because the cybersecurity inspector qualification program does not incorporate available resources for periodic refresher training. As a result, future inspections may be performed inefficiently and inconsistently due to knowledge gaps, undermining the effectiveness of the inspection program.

What Is Required

Expectations for Training and Training Qualifications should be Clearly Defined

Management Directive 10.77, "Employee Development and Training," states that the NRC's qualification programs are collaboratively designed to define training and qualification requirements for specific positions within the NRC program, regional, or corporate offices. These programs also set the requirements for refresher and continuing training to maintain employee qualifications. To participate on a cybersecurity inspection team, inspectors are required to complete the qualification program described in both IMC 1245, Appendix C-14, and IMC 1245, Appendix D-1, "Maintaining Qualifications," the latter of which contains the requirements for maintaining the IMC 1245, Appendix C-14 qualification.

The *Standards for Internal Control in the Federal Government* further states that management should set competence expectations for key roles and other roles as needed, ensuring that employees have the necessary knowledge, skills, and abilities, which are acquired through professional experience, training, and certifications, to achieve the entity's objectives.

What We Found

Expectations for Completing Refresher Training and Maintaining Training Qualifications are not Well-Defined

While the NRC has a qualification program for cybersecurity inspectors, the requirements for maintaining or refreshing knowledge are not well-defined. According to IMC 1245, Appendix D-1, inspectors must maintain cybersecurity qualification proficiency by attending the Cybersecurity Inspector Annual Counterpart meeting and participate in a minimum of one cybersecurity inspection per 3-year cycle. However, IMC 1245, Appendix D-1, does not contain any post-qualification requirements and only broadly suggests optional training to maintain qualifications.

Inspectors expressed to the OIG a desire for more targeted training in this area, stating that, aside from the periodic counterpart meetings, there is little follow-up after initial qualification, and the qualification program does not describe how inspections are currently performed.

Further, internal refresher training for cybersecurity inspectors and contractors is sporadic due to inspection schedules. In addition to cybersecurity inspections, regional inspectors plan and perform their qualified inspections year-round. The annual regional counterpart meeting allows the program office and regions to discuss lessons learned from the past inspection year and any controversial violations. It also provides an opportunity for training, but only occurs once a year. The NRC updates its advanced cybersecurity training as new cybersecurity information and technologies are learned. However, there is no requirement to retake any NRC training within the IMC 1245, Appendix C-14, journal to refresh or increase inspectors' cybersecurity knowledge with the most recent technical information.

Why This Occurred

The Cybersecurity Inspector Qualification Program does not Incorporate Available Training Resources as Periodic Refresher Training

While NSIR supports external training, staff noted that cybersecurity training outside the agency is costly, which could present a barrier to continuous learning. As such, staff rely on the agency's internal training. However, the qualification program does not incorporate Cyber SIFs or potential contractor-developed training.

Despite being recognized as an effective method for knowledge transfer between inspection staff and contractors, there are no requirements for inspectors to attend the Cyber SIFs after each cybersecurity inspection unless they are presenting the inspection findings. Specifically, in addition to the presenting inspection team, the only regional attendees required are the branch chiefs or a designee from each region. Although invitations to Cyber SIFs are sent to approximately 80 staff members, including all regional inspectors, the meeting is optional and many inspectors have scheduling conflicts due to other inspections, so attendance is often low. The OIG attended a Cyber SIF for the Beaver Valley Power Station cybersecurity inspection and noted that only four optional inspectors attended. Further, the Annual Cybersecurity Counterpart Meeting is not recorded, so inspectors cannot reference it if they are unable to attend the virtual meeting due to scheduling conflicts.

In addition, while the NRC relies on contractor employees for technical expertise, pertinent knowledge is not effectively shared with inspectors. NSIR is underusing its cybersecurity contract, which includes a task for the contractor to deliver quarterly virtual training sessions for cybersecurity inspectors. The contract includes

quarterly sessions on inspection techniques, common issues, cybersecurity, and digital forensics, but the agency has not requested their development due to contractor scheduling issues.

Why This Is Important

Knowledge Gaps can Reduce the Effectiveness and Efficiency of Cybersecurity Inspections

Undefined training requirements could lead to knowledge gaps and reduce the effectiveness and efficiency of future inspections. As the agency transitions from a performance-based to a risk-based regulatory model, clearer training requirements are essential. Clearer training expectations may help experienced and new inspectors perform more effectively, consistently, and efficiently.

Infrequent training prevents the agency from identifying potential knowledge gaps that should be addressed to ensure inspection requirements are evaluated consistently. Although the number of inspection findings has decreased since the cybersecurity baseline inspections began in January 2022, new issues continue to emerge at each site. With the shift to a 3-year inspection cycle, knowledge reinforcement is essential but may decline due to the increased time between inspections. At the same time, this extended frequency should provide the contractor with more opportunities to deliver quarterly training to NRC inspectors, as stated in the contract, keeping the inspectors abreast of the developments in the cybersecurity inspection program.

Recommendations

The OIG recommends that the EDO:

2.1. Update Inspection Manual Chapter 1245, Appendix D-1, to include periodic refresher training requirements for cybersecurity-qualified inspectors; and,

2.2. Define a schedule for contractor-led training (in-person or virtual) and ensure sessions are recorded and accessible.

3. The Cybersecurity Inspection Process Contains Redundant and Time-Consuming Tasks

The NRC should ensure regulatory actions are efficient, purposeful, and clearly tied to organizational goals to promote effective project management; however, the NRC's cybersecurity inspection process is too intensive and requires redundant, burdensome tasks. This occurred because the current inspection guidance lacks specificity and resource references that would promote efficiency and streamline inspections. As a result, the efficiency and effectiveness of current and future inspections could be negatively impacted, placing a burden on licensees.

What Is Required

Regulatory Actions should be Efficient, Purposeful, and Clearly Tied to Organizational Goals to Promote Effective Project Management

Project management, under the agency's Mission Statement Implementation Guidance, emphasizes a risk-informed approach where workstreams are clearly defined, milestones are tracked, and resources are allocated based on the safety or security significance of tasks. It encourages discontinuing low-impact efforts to focus on more critical issues, ensuring time and expertise are used effectively. Complementing this, the NRC's Principles of Good Regulation advocate for efficiency and clarity, which means that activities are consistent with the degree of risk reduction achieved and directly connect regulatory actions and agency goals.

What We Found

The Cybersecurity Inspection Process Requires Redundant and Burdensome Tasks

The current performance-based inspection model is redundant and time-consuming. IP 71130.10 requires substantial pre-on-site document review and intensive on-site activities to complete the inspection. RFIs often request excessive and redundant information on timelines that can be overwhelming for inspection teams to review and challenging for licensees to meet.

In the first part of the RFI process, the NRC typically requests that licensees provide abundant and sometimes repetitive information. Inspectors noted that the NRC already has some of that information, such as the cybersecurity plans, and it should not need to request it again. In addition, due to the tight inspection schedule,

contractors may be reviewing RFI responses for the next cybersecurity inspection while completing another inspection, which may make reviewing RFIs in a short amount of time an intensive task. In an OIG-administered licensee survey of operating reactor licensees, 9 out of 11 respondents stated the initial RFI includes unnecessary or redundant information, and some stated that providing the requested information required intensive resources.

In addition, licensees may be given unreasonable timelines to respond to the initial RFIs with bulk information. The OIG analyzed 109 initial RFIs issued for the cybersecurity baseline inspections and determined:

- 64 percent of RFIs were issued fewer than the standard 120 days prior to the on-site inspection; and,
- 46 percent of initial RFIs did not provide licensees the full 36 days to respond. For example, 13 initial RFIs requested a response within 20 days, and some of those requested a response in as little as eight days.

In addition, the third round of RFIs is often issued the Friday before the inspection begins, which is typically a nonworking day for licensee staff receiving them, limiting licensees' ability to prepare adequately.

Why This Occurred

Current Inspection Guidance Lacks Specificity and Resource References that would Promote Efficiency and Streamline Inspections

The inefficiencies and burdens identified in the cybersecurity inspection process stem from a lack of specificity in current inspection guidance and inconsistent use of available NRC resources. The agency is not using its own data resources to obtain licensee data efficiently and reduce licensee burden. Although the NRC has previously conducted comprehensive, programmatic reviews of licensee cybersecurity programs,[8] inspectors continue to request information that should already exist in NRC systems, such as the Agencywide Documents Access and Management System. Inspectors noted most programs have not made significant changes since cybersecurity full-implementation inspections were completed in 2021. The OIG acknowledges that inspectors cannot always rely on previously submitted documents and require confirmation that they have the most recent information. However, the RFI guidance does not ask inspection teams to first determine—for example, through consultation with the licensee or a review of data in

[8] The full-implementation inspection phase was completed between 2017 and 2021.

NRC systems—whether information has changed since the NRC reviewed the licensee's responses to the most recent initial RFI approximately two years earlier.

In addition, the guidance for issuing RFIs lacks enforceable timelines beyond the initial 120-day requirement. While the accompanying template provides suggested target dates for subsequent RFIs and licensee responses, these are often treated as flexible guidelines rather than firm expectations. Some inspectors may not refer to the guidance at all and instead modify prior RFIs in a manner that may not align with current guidance, contributing to inconsistent practices and compressed response windows. While the RFI template was recently revised to reduce the amount of information requested from licensees, it still refers to the current RFI guidance, which lacks specificity and retains the original information request list.

Why This Is Important

Process Affects the Efficiency and Effectiveness of Cybersecurity Oversight

The current inspection process affects both the efficiency and effectiveness of cybersecurity oversight. Compressed timelines and redundant information requests hinder inspection planning. Although the agency is moving toward a triennial inspection schedule that relies on fewer contractor employees and simplifies requirements, this shift will increase the volume of documentation to review in each cycle. While the current inspection leads are familiar with the inspection requirements, the agency should consider that many cybersecurity inspectors are relatively inexperienced and may need more time to select inspection samples effectively.

The RFI process has also resulted in an added burden on the licensees, who may struggle to compile and submit large volumes of documentation on short notice. While inspectors noted that licensees consistently provide the RFI response information by the deadlines, early and targeted communication with licensees has been shown to improve inspection outcomes by allowing better preparation and more focused reviews. For example, during the Beaver Valley inspection in 2025, the third RFI was issued on Wednesday (instead of Friday) before the on-site inspection, allowing licensees two extra days to prepare their responses to the inspectors for the following Monday's on-site inspections. Beaver Valley personnel reported feeling better prepared overall by the end of the inspection and expressed appreciation for the inspection's structure, early communication, and clarity. Inspectors were able to identify potential issues early and concentrate on risk-significant areas. This

example illustrates the value of timely, targeted information requests and structured planning in achieving both regulatory objectives and operational efficiency.

Recommendations

The OIG recommends that the EDO:

3.1. Revise the request for information guidance to require inspectors to identify the most current cybersecurity program documents already in the NRC's possession before issuing the initial request, and to clearly communicate target dates for both issuing requests and receiving licensee responses.

4. NRC Staff Members did not Always Accurately Report their Time Spent on Cybersecurity Inspection-Related Activities

Time and Labor reporting should be accurate and verified prior to submission in the Human Capital Management (HCM) Cloud system. The OIG found, however, that inspectors' approved hours were not properly recorded in HCM Cloud. This occurred due to improper oversight of reported time and unclear guidance on when to use the oversight codes. As a result, HCM Cloud contained incorrect data that could negatively affect the identification and budgeting of necessary resources for cybersecurity inspection activities.

What Is Required

Time and Labor Reporting should be Accurate and Verified Prior to Submission

The NRC uses the HCM Cloud system to collect time and attendance data for payroll purposes, budget formulation and execution, operations and workload planning, resource expenditure tracking, licensee billing, and fee-related cost management. The NRC's Labor Reporting and Policy Guidance states labor costs are tracked using Cost Activity Codes (CACs) and Enterprise Project Identifier (EPID) codes. CACs are six-digit codes that define the type of work performed, such as licensing or inspection activities, with examples including CAC 000741, the fee-billable code for cybersecurity inspections, and CAC A11020, a non-fee billable code used for indirect efforts related to security program activities not tied to a specific docket. EPIDs are alphanumeric codes that identify each project by type, year, and sub-type.

For billable work, staff must record time in HCM Cloud using a CAC-Docket Number-EPID labor string: the CAC specifies the activity, the EPID represents the project, and the docket number identifies the licensee facility. This structure enables the agency to track employee use by office and region for projects, licensing actions, and inspections. Employees are responsible for accurately recording their time in HCM Cloud using the correct project and activity codes, while approving officials, typically first-line supervisors and managers, must verify and approve reported time in accordance with agency policies.

The NRC's Labor Reporting Policy & Guidance emphasizes the use of EPIDs linked to CACs to enhance labor tracking and cost reporting. This structure enables accurate tracking by office or region, supports cost-per-output analysis, and improves labor data accuracy through standardized reporting and better controls. It also facilitates timely responses to congressional inquiries, increases transparency for licensees, supports multi-budget and multi-docket project tracking, and allows full-cost reporting by capturing both labor and non-labor expenses.

What We Found

Inspectors' Hours were not Properly Recorded in HCM Cloud

The OIG's analysis of time and labor reported in HCM Cloud between January 1, 2022, and June 30, 2025, revealed that eight inspectors who performed cybersecurity inspection-related activities across three regions had not properly charged their time to CAC A11020, the CAC for security oversight activities. Rather, those inspectors had been charging their time to CAC A11018, which is used for safety-related oversight activities. Although some of those inspectors were not cybersecurity inspection team members, their time should have been allocated to CAC A11020 if they attended a Cyber SIF as an observer or completed training for the cybersecurity inspector qualification.

Furthermore, the time and labor reported to HCM Cloud for CAC 000741 between January 1, 2022, and June 30, 2025, revealed that one cybersecurity inspection reported 14 hours for completion, which was questionable based on the estimated 70 hours it takes to complete an inspection, according to IP 71130.10. Upon review, the OIG determined the inspector erroneously charged 29 hours of his time to CAC 000980, the fee-billable code for security inspection preparation and documentation. See Appendix B for the description of each CAC used by the inspectors during the period reviewed.

Why This Occurred

Improper Oversight of Reported Time and Unclear Guidance on Oversight Activity Codes

Management did not identify the staff's incorrect timekeeping for inspection activities. As background, when the cybersecurity program was initially established, the regional inspection groups that performed fire protection and electrical inspections, which are safety inspections, inherited cybersecurity inspections. These inspections are performed at various sites throughout the calendar year, and preparatory activities may overlap. Inspectors may have been unaware of the proper CAC to use for oversight activities or may have used the safety oversight CAC out of convenience.

Two branch chiefs acknowledged their inspectors had not been charging their indirect cybersecurity inspection activities to CAC A11018. They also stated that when approving time, their focus is on ensuring accurate billing to licensees and determining whether there are abnormalities in the time codes used (e.g., overtime, comp time, and special travel time). These branch chiefs noted they periodically need to remind their staff to use the proper codes.

One branch chief stated that there is a lack of clear guidance on when to use the cybersecurity-related oversight codes. The OIG determined that the non-billable CAC guidance generally describes when the oversight CACs should be used, but may benefit from additional clarity. The Cyber SIF guidance also lacks CAC guidance for Cyber SIF participants. The branch chief informed the OIG that the agency may consider adding more granularity to these oversight codes, which could be used in project management and role-based performance metrics under the new appraisal system starting in Fiscal Year 2026. The NRC is also undergoing a mission-related reorganization, and this reorganization may require the agency to take additional steps to achieve consistency in using cybersecurity-related CACs.

The OIG also found that an inspector applied the wrong fee-billable CAC for a 2024 cybersecurity inspection, and this error was not corrected in the HCM Cloud System at the time of review and approval. Although the wrong CAC was used, the OIG confirmed the NRC did not overbill or underbill any licensee for cybersecurity inspections in this instance or in any other instance involving erroneous CAC usage that the OIG reviewed as part of this audit.

Why This Is Important

Incorrect Data Negatively Affect the NRC's Ability to Identify and Budget the Necessary Resources for Cybersecurity Inspection Activities

Incorrect data could lead to improper budget formulation, understating the actual resources dedicated to security oversight activities, and overstating the resources dedicated to safety oversight activities. IP 71130.10 uses resource estimates to determine how much time may be required to complete inspections, ranging from 63 to 77 hours. Inaccurate reporting to the wrong fee-billable code could impact those resource estimates and lead to misrepresentations of the time it takes to complete direct inspections. Inaccurate reporting could also result in underpayments or overpayments of fees by licensees.

The Nuclear Energy Innovation and Modernization Act requires the NRC to recover, to the maximum extent practicable, its total budget authority for the fiscal year, not including budget authority for excluded activities. Consistent with this law and other authorities, the NRC charges licensees hourly rates for fee-billable activities, and the agency recovers these fees based on inspectors' reported time and labor. Although during this audit the OIG did not identify any instance when licensees were overbilled or underbilled for cybersecurity baseline inspections, improper coding could nonetheless lead to undercharging or overcharging licensees.

Recommendations

The OIG recommends that the EDO:

4.1. Train staff on the correct Cost Activity Codes for reporting fee-billable and non-billable cybersecurity inspection activities within the Human Capital Management Cloud System;

4.2. Finalize the Cyber Security Issues Forum Draft Charter to include the Cost Activity Codes used by staff members when participating in or observing meetings;

4.3. Develop clear guidance on the appropriate use of security oversight Cost Activity Codes; and,

4.4. Develop and implement Enterprise Project Identifier codes for inspection oversight activities to improve tracking of safety and security related oversight activities.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

The OIG recommends that the Executive Director for Operations:

1.1. Develop and issue supplemental guidance clarifying the expected implementation of cybersecurity controls, the interpretation of requirements, and methods for evaluating control effectiveness;

1.2. Update Inspection Procedure 71130.10 to clarify the Cyber Security Issues Forum process and its potential impacts on findings and violations;

2.1. Update Inspection Manual Chapter 1245, Appendix D-1, to include periodic refresher training requirements for cybersecurity-qualified inspectors;

2.2. Define a schedule for contractor-led training (in-person or virtual), and ensure sessions are recorded and accessible;

3.1. Revise the request for information guidance to require inspectors to identify the most current cybersecurity program documents already in the NRC's possession before issuing the initial request, and to clearly communicate target dates for both issuing requests and receiving licensee responses;

4.1. Train staff on the correct Cost Activity Codes for reporting fee-billable and non-billable cybersecurity inspection activities within the Human Capital Management Cloud System;

4.2. Finalize the Cyber Security Issues Forum Draft Charter to include the Cost Activity Codes used by staff members when participating in or observing meetings;

4.3. Develop clear guidance on the appropriate use of security oversight Cost Activity Codes; and,

4.4. Develop and implement Enterprise Project Identifier codes for inspection oversight activities to improve tracking of safety and security related oversight activities.

V. NRC COMMENTS

Agency management reviewed the discussion draft version of this report and did not have comments. The NRC waived the exit conference with the OIG on May 12, 2026.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The audit objective was to determine if the NRC's cybersecurity inspection program for operating nuclear plants is robust and adaptive to evolving cyber threats.

Scope

The audit assessed the implementation of the cybersecurity inspection program for operating reactor plant facilities, emphasizing the efficiency and effectiveness of inspection processes, the training qualifications and capabilities of regional inspectors, and the sufficiency of resources allocated to support cybersecurity inspections. We conducted this performance audit at NRC headquarters in Rockville, Maryland, from May 2025 to February 2026.

We reviewed and analyzed internal controls related to the audit objective; specifically, the components of the control environment, risk assessments, control activities, information and communication, and monitoring. Within those components, the OIG reviewed the principles of:

- Overseeing the entity's internal control system;
- Demonstrating a commitment to recruit, develop, and retain competent individuals;
- Defining objectives clearly to enable the identification of risks and define risk tolerances;
- Identifying, analyzing, and responding to risks related to achieving the defined objectives;
- Identifying, analyzing, and responding to significant changes that could impact the internal control system;
- Designing control activities to achieve objectives and respond to risks;
- Designing the entity's information system and related control activities to achieve objectives and respond to risks;
- Implementing control activities through policies;
- Using quality information to achieve the entity's objectives;
- Internally communicating the necessary quality information to achieve the entity's objectives;

- Externally communicating the necessary quality information to achieve the entity's objectives;
- Establishing and operating monitoring activities to monitor the internal control system and evaluate the results; and,
- Remediating identified internal controls deficiencies on a timely basis.

Methodology

The OIG reviewed relevant criteria for this audit, including:

- 10 C.F.R. section 73.54;
- RG 5.71, Revision 1, *Cybersecurity Programs for Nuclear Power Reactors*;
- NEI 08-09, Revision 6, *Cyber Security Plan for Nuclear Power Reactors*;
- IP 71130.10, "Cybersecurity";
- *Guidance Document for Development of the Request for Information and Notification Letter for IP 71130.10 Cyber Security Inspection*;
- Cybersecurity Issues Forum Charter;
- NRC's Cybersecurity Inspector Training and Qualification Requirements, Training Course Materials, and Knowledge Management Resources;
- Cybersecurity contract Statement of Work;
- NRC Strategic Plan, Fiscal Years 2022-2026; and,
- NRC's Time and Labor Reporting Guidance.

The OIG interviewed NRC staff and management to understand their responsibilities in overseeing the agency's cybersecurity inspection program, including the development and maintenance of program guidance, staff training, subject matter expertise, and contract management. The OIG also conducted interviews with NRC regional inspectors and contractor employees to gain insight into the cybersecurity inspection program and to identify current challenges and opportunities for improvement. In addition, the OIG distributed a voluntary survey to licensees to gather feedback on potential improvements to the cybersecurity inspection program's guidance, as well as its planning and implementation processes.

The OIG analyzed the Cybersecurity Inspection Program to assess its effectiveness and efficiency. Specifically, we reviewed RFI issuance and response timelines, inspection report metrics, Cyber SIF worksheets, and cybersecurity inspection findings and violations. We also evaluated the training and qualifications of regional inspectors to verify the level of expertise and technical proficiency required for their roles, and we examined the time, labor costs, and activities involved in conducting the inspections. In August 2025, the OIG visited Beaver Valley Power Station in

Shippingport, Pennsylvania, to observe a cybersecurity inspection, following the inspection process from initial planning through final report issuance.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Throughout the audit, auditors considered the possibility of fraud, waste, and abuse in the program.

The audit was conducted by Mike Blair, Team Leader; Janelle Davis, Audit Manager; Manpreet Sandhu, Auditor; Salma Rahaman, Management Analyst; and, Pete Snyder, Senior Technical Advisor.

TIME AND LABOR REPORTING REQUIREMENTS

For time and labor reporting, the NRC categorizes activities as either mission direct or mission indirect:

- Mission direct time refers to the performance of core work activities that directly support the agency's mission—providing reasonable assurance of adequate protection of public health and safety, promoting the common defense and security, and protecting the environment; and,
- Mission indirect time includes activities that support the mission direct work, such as administrative or preparatory tasks.

Employees must accurately record their time in HCM Cloud using the appropriate project and activity codes. CACs are six-digit identifiers that specify the type of work performed (e.g., licensing or inspection). These codes enable tracking labor costs for mission-related activities, accurate fee billing for hours charged, and effective budgeting of resources across business lines.

Table 2 defines the CACs associated with cybersecurity inspections and lists those used by employees and inspectors who performed direct and indirect cybersecurity inspection activities between January 2022 and June 2025.

Table 2: Definitions for CACs Used for Cybersecurity Inspection Activities Between January 1, 2022, and June 30, 2025

CAC	Title	Description
000741	FB-OR-IP-7113010P-Cyber Security	Fee-billable code for on-site cybersecurity inspections
000980	FB-OR-Security Inspection Preparation-Documentation	Fee-billable code for preparing security inspection documentation
A11018	NB-OP RX-Oversight-Inspections	NON-FEE Billable – Indirect efforts of HQ and regional inspection program staff expended on inspection and assessment program activities

		related to the safety performance of nuclear facilities but not pertaining to a docket (not otherwise captured using other billable activity codes or inspection report numbers).
A11020	NB-OP RX-Oversight-Security	NON-FEE BILLABLE – Indirect efforts related to the Security program activities not pertaining to a docket (not otherwise captured using other billable activity codes or inspection report numbers) associated with Security program. Examples include program assessments/enhancements, support for new or revised regulatory requirements program oversight/activities, force-on-force activities, cyber-security activities, inspection support activities, office/regional instruction revisions, contract administration activities, knowledge transfer/mentoring and other Office/Regional Security support.

Source: NRC's Time & Labor Reporting Policies

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Online:	Hotline Form
Telephone:	1.800.233.3497
TTY/TDD:	7-1-1, or 1.800.201.7165
Address:	U.S. Nuclear Regulatory Commission Office of the Inspector General Hotline Program Mail Stop O12-A12 11555 Rockville Pike Rockville, Maryland 20852

COMMENTS AND SUGGESTIONS

If you wish to provide comments on this report, please email the OIG using this link.

In addition, if you have suggestions for future OIG audits, please provide them using this link.

NOTICE TO NON-GOVERNMENTAL ORGANIZATIONS AND BUSINESS ENTITIES SPECIFICALLY MENTIONED IN THIS REPORT

Section 5274 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, amended the Inspector General Act of 1978 to require OIGs to notify certain entities of OIG reports. In particular, section 5274 requires that, if an OIG specifically identifies any non-governmental organization (NGO) or business entity (BE) in an audit or other non-investigative report, the OIG must notify the NGO or BE that it has 30 days from the date of the report's publication to review the report and, if it chooses, submit a written response that clarifies or provides additional context for each instance within the report in which the NGO or BE is specifically identified.

If you are an NGO or BE that has been specifically identified in this report and you believe you have not been otherwise notified of the report's availability, please be aware that under section 5274 such an NGO or BE may provide a written response to this report no later than 30 days from the report's publication date. Any response you provide will be appended to the published report as it appears on our public website, assuming your response is within the scope of section 5274. Please note, however, that the OIG may decline to append to the report any response, or portion of a response, that goes beyond the scope of the response provided for by section 5274. Additionally, the OIG will review each response to determine whether it should be redacted in accordance with applicable laws, rules, and policies before we post the response to our public website.

Please send any response via email using this link. Questions regarding the opportunity to respond should also be directed to this same address.