FINAL SUPPORTING STATEMENT
FOR
SUSPICIOUS ACTIVITY REPORTING USING THE
PROTECTED WEB SERVER (PWS)

(3150-0219)

EXTENSION

Description of the Information Collection

The Protected Web Server (PWS) enables the U.S. Nuclear Regulatory Commission (NRC) to securely communicate sensitive information to licensees and strengthen long-term relationships with Federal, State, and local organizations that share responsibilities for protecting nuclear facilities and activities and responding to incidents. PWS serves as the NRC's repository for storing security-related information reported to the NRC.

Under the PWS program, NRC license holders and applicants subject to Title 10 of the *Code of Federal Regulations* (10 CFR) 73.1215, "Suspicious Activity Reports," paragraphs (d), (e), and (f), are required to report suspicious activities related to their facility, material, or shipping operations. Entities not subject to this requirement may voluntarily submit security-related reports in response to NRC advisories. Entities that may voluntarily report include but are not limited to: applicants for part 50 or 52 licenses; holders of construction permits under 10 CFR part 50; fuel fabrication facilities; uranium conversion/deconversion facilities; and holders of certificates of compliance under 10 CFR part 72. Each report, whether required or voluntary, provides details about a specific suspicious activity (e.g., suspicious person, manned or unmanned aircraft flyovers) and the actions taken by the reporting organization to address the suspicious activity.

A. JUSTIFICATION

1. Need for and Practical Utility of the Collection of Information

The mission of the NRC is to regulate nuclear reactors, materials, and waste facilities in a manner that protects public health and safety, promotes common defense and security, and protects the environment. Security at nuclear facilities has long been the subject of NRC regulatory oversight.

Following the September 11, 2001 terrorist attacks, custodians of the Nation's critical infrastructure reassessed the adequacy of security measures at their facilities. To address changes in the threat environment, the NRC undertook a comprehensive review of its safeguards and security programs to identify prompt actions and long-term enhancements that would provide reasonable assurance of adequate protection of nuclear facilities nationwide.

The PWS supports the Nationwide Suspicious Activity Reporting (SAR) Initiative which began in 2008, by serving as the NRC's contribution to centralizing suspicious activity reporting. This initiative helps assess national trends across industries and critical infrastructure.

NRC licensees are encouraged to report suspicious activity as outlined in the 2005 Department of Homeland Security (DHS)/Federal Bureau of Investigation (FBI)

suspicious activity reporting guide[1] and the 2009 DHS cyber-security recommended practice guide.[2] The NRC has also issued two information advisories (IAs) providing guidance on suspicious activity reporting: IA-04-08[3] and IA-13-01.[4]

These reports contain sensitive information and are not publicly available. Sensitive information from these reports is added to the PWS and shared with authorized nuclear industry officials and Federal, State, and local government agencies.

2. Agency Use of Information

Analysts in the NRC's Office of Nuclear Security and Incident Response (NSIR) review threat-related information to evaluate and assess potential threats to the NRC and its licensees. Analysts coordinate threat-related information with the FBI, DHS, and other national-level intelligence agencies to assess threat levels. The PWS is also used as a vehicle to communicate threat-related information to NRC licensees.

3. Reduction of Burden Through Information Technology

There are no legal obstacles to reducing the burden associated with this information collection. The NRC encourages respondents to use information technology when beneficial.

The NRC issued *Guidance for Electronic Submissions to the NRC*, which provides direction for electronic transmission and submittal of documents. Electronic transmission can be accomplished via the Electronic Information Exchange process (available on the NRC's "Electronic Submittals" Web page), optical storage media (e.g., CD-ROM, DVD), secure facsimile, telephone, or e-mail. Currently, all responses (i.e., security reports from NRC licensees) are submitted via telephone.

4. Effort to Identify Duplication and Use Similar Information

No sources of similar information are available. There is no duplication of requirements.

5. Effort to Reduce Small Business Burden

One of the main purposes of this effort is to gather necessary information without imposing significant additional burden on small businesses. Per the recent implementation of the Enhanced Weapons Rule (EWR) in January 2025, reporting suspicious activity is now mandatory for all NRC licensees, and the number of questions on the information collection will be kept to a minimum. Small businesses, as well as the NRC, will benefit from the government's increased responsiveness to their needs.

---

[1] "Terrorist Threats to the U.S. Homeland: Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators," DHS/FBI, January 2005.
[2] "Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability," DHS, October 2009.
[3] "Reporting Suspicious Activity Criteria," NRC, October 2004.
[4] "Updated Criteria to Reporting Suspicious Activity Associated with Cyber Security Incidents," NRC, January 2013.

6. Consequences to Federal Program or Policy Activities if the Collection is Not Conducted or is Conducted Less Frequently

Per the EWR, NRC licensee suspicious activity reporting is mandatory within established timelines from when a suspicious activity occurs for licensees subject to 10 CFR 73.1215. This reporting is necessary to allow the NRC to provide timely intelligence assessments to prevent or mitigate potential threats to the NRC or its licensees.

Failure to collect suspicious activity information would significantly impair the NRC's ability to analyze and assess threats to its licensees, potentially resulting in radiological sabotage, theft, or diversion of special nuclear materials. It would also create a gap in threat-related information reporting from the nuclear sector for the SAR Initiative.

7. Circumstances Which Justify Variation from Office of Management and Budget Guidelines

There is no requirement for NRC licensees to report suspicious activities on a routine schedule. Rather, licensees report suspicious activities as they occur, which may result in reporting more often than an established periodicity (e.g., quarterly).

Immediate reporting is necessary to allow the NRC to provide timely intelligence assessment to prevent or mitigate potential threats. Additionally, NRC licensees are directed to report suspicious activities as appropriate to State and local law enforcement authorities, FBI, DHS, Federal Aviation Administration, and other Federal agencies.

8. Consultations Outside the NRC

Opportunity for public comment on the information collection requirements for this clearance package was published In the Federal Register on May 21, 2026 (91 FR 29988). Four separate licensees under 10 CFR Part 50 (Three-Mile Island, Byron, Dresden, and Seabrook) were contacted via email. No comments were received in responses to these consultations.

9. Payment or Gift Respondents

Not applicable.

10. Confidentiality of Information

Confidential and proprietary information is protected in accordance with NRC regulations at 10 CFR paragraphs 9.17(a) and 2.390(b). Suspicious activity reports may contain personally identifiable information (PII) or other sensitive but unclassified information about the facility, security posture, countermeasures, and potential vulnerabilities. For example, information may

relate to identifying an individual or vehicle involved in a suspicious activity, such as name, address, date of birth, vehicle make and model, license plate, or vehicle identification number. Access to PII and other sensitive information is limited to select individuals within the NRC, FBI, and DHS, and is redacted for all other PWS users.

PWS administrators apply the principle of least privilege when assigning access rights. All users (including NRC staff, authorized nuclear industry officials, and Federal, State, and local government agencies), are assigned role-based access rights based on their need-to-know. PWS users must accept terms of service before being granted an account. FBI and DHS representatives are the only external users with role-based access rights to any PII in the PWS.

Currently, approximately 43 representatives from the FBI and DHS have access to the PWS. These individuals represent various offices, task forces, and directorates related to weapons of mass destruction, critical infrastructure, and nuclear and radiological issues. All requests from the FBI and DHS are reviewed and approved by NSIR before creation.

In December 2020, a Privacy Impact Assessment was performed for the system. A System of Records Notice is not required because the system is not searchable for PII by users. Searchable fields for suspicious activities include: incident ID, date, region, reporting organization, site/licensee name, report category, current phase, status, and last updated date. To avoid any potential issues with searching for PII, the full-text search feature is limited to Communication Documents and Cyber-Related Documents Views.

11. Justification for Sensitive Questions

No questions of a sensitive nature are contained in any of the associated information collection requirements.

12. Estimated Burden and Burden Hour Cost

The NRC staff estimates that 56 licensees will annually submit 65 reports through the PWS, and that each report will require 1 hour to prepare and submit. Staff also estimates 30 third-party notifications by reporting licensees that will require 15 minutes each. The total licensee burden for this information collection is 72.5 hours (65 reports x 1 hour = 65 hours and 30 reports x 0.25 hour = 7.5 hours) at a cost of $11,165 (72.5 hours x $154/hour) (see Table 1).

The NRC’s average labor rate of $154 per hour for FY 2026 was used to calculate burden costs to the public because it aligns with 2024 Bureau of Labor Statistics data showing comparable hourly mean wages across five key occupational groups (executives, management, technical staff, licensing staff,

and physicists) within the nuclear industry.

13. Estimate of Other Additional Costs

    There are no additional costs.

14. Estimated Annualized Cost to the Federal Government

    Annual costs to the NRC include staff hours and contractual support:
    Staff Hours = 500 hours/year, at $154/hour = $77,000
    Contractual Support = $192,000 per year
    TOTAL COST = $269,000/year

15. Reasons for Change in Burden or Cost

    The estimated burden would increase from 78 responses and 58 hours to 95 responses and 72.5 hours, an increase of 17 responses and 14.5 hours.

    The NRC expects an increase in reports submitted annually using the PWS due to continuing implementation of the EWR. In addition, the NRC staff updated the estimated burden per response from two hours to one hour due to a PWS update that allows for a more streamlined process.

    Finally, the rate used to calculate burden cost decreased from $290 to $154/hour.

16. Publication for Statistical Use

    Due to the sensitivity of the information contained in the PWS, all information is considered OFFICIAL USE ONLY and will not be shared publicly.

17. Reason for Not Displaying the Expiration Date

    Not applicable.

18. Exceptions to the Certification Statement

    None.

B. COLLECTIONS OF INFORMATION EMPLOYING STATISTICAL METHODS

Not applicable.

TABLE 1

ANNUALIZED REPORTING BURDEN

	Total No. of Responses	Burden Hours per Response	Total Annual Reporting Burden (hours)
Estimated Mandatory Suspicious Incident Reporting for CY 2026	65	1	65
Voluntary third-party notification	30	.25	7.5
Total	95		72.5

TOTAL BURDEN HOURS: 72.5 hours (65-hours reporting + 6.5 hours third party notification + 0 hours

recordkeeping) TOTAL BURDEN HOUR COST:$11,165 (72.5 hours x

$154/hour)

ANNUAL RESPONDENTS: 65 respondents

RESPONSES: 95 responses (65-reporting responses + 30 third party responses)