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 fulfill its mission of communicating sensitive information to licensees and developing more formal, long-term relationships with Federal, State, and local organizations—who, along with the NRC, have responsibilities for protecting nuclear facilities and activities and responding to incidents.

Under the PWS program, nuclear power reactor licensees voluntarily provide security reports as a result of various advisories that the NRC issues. These licensees provide the majority of the reports, but other NRC licensed entities that may voluntarily send reports include fuel facilities, independent spent fuel storage installations, decommissioned power reactors, power reactors under construction, research and test reactors, agreement States, non-agreement States, as well as users of byproduct material (e.g., departments of health, medical centers, universities, steel mills, well loggers, and radiographers). Each report that the NRC receives provides details about a specific security incident that occurs (e.g., suspicious person, suspicious activity, flyovers) and the actions that the reporting organization is taking to address the incident.

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 the health and safety of the public, promotes the common defense and security, and protects the environment. Security at nuclear facilities across the country has long been the subject of NRC regulatory oversight.

The terrorist attacks on the U.S. on September 11, 2001, brought to light a new and more immediate threat to our country. All custodians of the Nation's critical infrastructure needed to reconsider decisions made earlier about the adequacy of security at the facilities under their charge. To cope with these changes in the threat environment, the NRC undertook a reassessment of its safeguards and security programs to identify prompt actions and long-term enhancements that would raise the level of security at the nuclear facilities across the country.

The PWS fulfills a valuable need in relation to the Nationwide Suspicious Activity Reporting (SAR) Initiative which began in 2008. PWS is the NRC's contribution to this important national initiative to centralize suspicious activity reporting in the interest of assessing 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. This sensitive information 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 the level of threat. 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 it would be beneficial to them.

The NRC issued *Guidance for Electronic Submissions to the NRC*, which provides direction for the electronic transmission and submittal of documents. Electronic transmission and submittal of documents can be accomplished via the following avenues: the Electronic Information Exchange process, which is available from the NRC's "Electronic Submittals" Web page; by optical storage media (e.g., CD-ROM, DVD); by facsimile; by telephone; or by e-mail. It is estimated that none of the potential responses (i.e., security reports from NRC licensees) are filed electronically and 100 percent are reported to the NRC 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 information needed without putting significant additional burden on small businesses. Reporting suspicious incidents is voluntary for all respondents, and the number of questions on the information collection will be kept to a minimum. However, small businesses, as well

[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 Cyber-security 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.

as the NRC, will benefit by the government's increased responsiveness to their needs.

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

   NRC licensees report this information voluntarily on an ad-hoc basis, as suspicious incidents occur. 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.

   If suspicious incident information was not collected, it would negatively affect the NRC's ability to analyze threats to its licensees. It would also create a void in threat-related information pertaining to the nuclear sector in the National Security Environment/SAR program.

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

   There exists no requirement for NRC licensees to report suspicious incidents on a routine reporting schedule. Rather, licensees are encouraged to voluntarily report suspicious incidents on an as-needed basis as security incidents occur and/or as security incidents are identified, which may lead to reporting more often than quarterly. This immediate reporting is necessary to allow the NRC to provide timely intelligence assessment to prevent or mitigate potential threats to the NRC or its licensees.

8. Consultations Outside the NRC

   Opportunity for public comment on the information collection requirements for this clearance package was published In the *Federal Register (FR)* on December 9, 2019 (84 FR 67298). The NRC contacted four potential respondents vie e-mail to request feedback on the information collection. All four potential respondents were licensees that fall within the scope of Title 10 of the *Code of Federal Regulations* (10 CFR) Part 95. No comments were received in responses to these consultations.

9. Payment or Gift to Respondents

   This section is 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 incident reports may contain personally identifiable information (PII) or other sensitive but unclassified information about the facility, security posture, security counter-measures, and other potential vulnerabilities. For example, information may relate to identifying an individual or vehicle involved in a suspicious incident, such as: name, address, date of birth, vehicle make and model, license plate, vehicle identification number, etc. Access to PII and other sensitive but unclassified information is limited to select individuals within the NRC and FBI, and is redacted for all other PWS users.

PWS administrators use the principle of least privilege when assigning access rights to PWS users. All users, including the NRC staff; authorized nuclear industry officials; and Federal, State, and local government agencies, are assigned role-based access rights in PWS based on their need-to-know. PWS users are also required to accept terms of service before being granted an account in the PWS. The NRC will not be able to ensure proper use of information by external users beyond limiting access based on need-to-know. FBI representatives are the only other users outside of the NRC that will have role-based access rights to any PII in the PWS.

To date, the NRC has approximately 20 representatives from the FBI who have access to the PWS. These individuals are not from a specific office within the FBI; rather, they represent a variety of FBI offices, task forces, and directorates related to weapons of mass destruction, critical infrastructure, and nuclear and radiological issues. All requests from the FBI for accounts in the PWS are reviewed and approved by NSIR before being created. .

A Privacy Impact Assessment was performed by the agency for the system in August 2011. A System of Records Notice is not required for this system because it is not searchable by PII. The only searchable fields for suspicious incidents are as follows: incident ID, date, region, reporting organization, site/licensee name, report category, current phase, status, and last updated (date). In order to avoid any potential issues with searching for PII, the full-text search feature is limited to the 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 assumes a $275 hourly rate for licensees to calculate their estimated hourly cost burden. The $275 hourly rate is based on the NRC's fee for hourly rates as noted in 10 CFR section 170.20, "Average cost per professional staff-hour." For more information on the basis of this rate, see the Revision of Fee Schedules; Fee Recovery for Fiscal Year 2018 (83 FR 29622, June 25, 2018).

The NRC staff estimates that 62 licensees will annually submit 124 reports through the PWS, and that each report will require 2 hours to prepare and submit. The total licensee burden for this information collection is 248 hours (124 reports x 2 hours = 248 hours) at a cost of $68,200 (248 hours x $275/hour) (see Table 1).

13. Estimate of Other Additional Costs

There are no additional costs.

14. Estimated Annualized Cost to the Federal Government

    The annual costs to the NRC include staff hours and contractual support:

    Staff Hours = 1,000 hours per year, at $275/hour = $275,000
    Contractual Support = $140,000 per year = prior year cost (beginning with $126,435 + approximately 5% for the costs of inflation and information technology modernization per year)
    TOTAL COST = $415,000

15. Reasons for Change in Burden or Cost

    There has been no change in the burden or the number of responses; however, the respondent cost increased due to the increase in the fee rate from $265 to $275/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

    This section is not applicable.

18. Exceptions to the Certification Statement

    None.

B. COLLECTIONS OF INFORMATION EMPLOYING STATISTICAL METHODS

This section is not applicable.

TABLE 1

ANNUALIZED REPORTING BURDEN

Section	No. of Respondents	Responses per Respondent	Total No. of Responses	Burden Hours per Response	Total Annual Reporting Burden (hours)
Voluntary Suspicious Incident Reporting for CY 2018	62	2	124	2	248

TOTAL BURDEN HOURS: 248 hours (248 hours reporting + 0 hours third-party notification + 0 hours recordkeeping)

TOTAL BURDEN HOUR COST: $68,200 (248 hours x $275/hour)

ANNUAL RESPONDENTS: 62 respondents (none required)

RESPONSES: 124 responses (124 reporting responses + 0 third-party responses + 0 recordkeepers)