1FINAL SUPPORTING STATEMENT
FOR

SUSPICIOUS ACTIVITY REPORTING
USING THE PROTECTED WEB SERVER (PWS)
(3150-XXXX)
NEW

Description of the Information Collection

The mission of the Nuclear Regulatory Commission (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, dating back to the 1970's.

The terrorist attacks on the United States 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.

In 2003, with the assistance of other Federal agencies, the NRC developed a database of reported security incidents, referred to as the Security Information Database (SID), which has since been renamed the Protected Web Server (PWS). Under this program, licensees voluntarily provide security reports as a result of advisories that NRC issues. Nuclear power reactor licensees provide the majority of reports, but other 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 NRC receives provides details about a specific security incident that has occurred (e.g., suspicious person, suspicious activity, flyovers) and the actions that the reporting organization is taking to address the incident. These reports are considered sensitive information and are handled accordingly. This information is added to PWS and shared with authorized nuclear industry officials and Federal, State, and local government agencies.

A. JUSTIFICATION

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

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

Further, PWS fulfills a valuable need in relation to the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) 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 providing guidance on suspicious activity reporting: IA-04-08[3] and IA-13-01[4].

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. 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. NRC issued a regulation on October 10, 2003 (68 FR 58791), consistent with the Government Paperwork Elimination Act, which allows its licensees, vendors, applicants, and members of the public the option to make submissions electronically via CD-ROM, e-mail, special Web-based interface, or other means. It is estimated that approximately 100% of the potential responses are filed electronically.

4. Effort to Identify Duplication and Use Similar Information

No sources of similar information are available. There is no duplication of requirements. NRC has in place an ongoing program to examine all information collections with the goal of eliminating all duplication and/or unnecessary information collections.

5. Effort to Reduce Small Business Burden

Not applicable.

---

[1][1] "Terrorist Threats to the U.S. Homeland: Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators," DHS/FBI, January 2005.

[2][2] "Recommended Practice: Developing an Industrial Control Systems Cyber-security Incident Response Capability," DHS, October 2009.

[3][3] "Reporting Suspicious Activity Criteria," NRC, October 2004.

[4][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

   Nuclear licensees report this information voluntarily on an ad-hoc basis, as suspicious incidents occur. This immediate reporting is necessary to allow NSIR to provide timely intelligence assessment 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 (NSE) / SAR Program.

7. Circumstances Which Justify Variation from OMB Guidelines

   There exists no requirement for 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 NSIR to provide timely intelligence assessment to prevent or mitigate potential threats to the NRC or its licensees.

8. Consultations Outside the NRC

   A 60-day public comment period was provided regarding these information collection requirements described in this clearance package. The Federal Register notice was published on August 8, 2013 (78 FR 48501). No comments were received. In addition, a second opportunity for comment was published on November 29, 2013 (78 FR 71673).

9. Payment or Gift to Respondents

   Not applicable.

10. Confidentiality of Information

    Confidential and proprietary information is protected in accordance with NRC regulations at 10 CFR 9.17(a) and 10 CFR 2.390(b). Suspicious incident reports may contain 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 & model, license plate, VIN, 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 used the principle of least privilege when assigning access rights to PWS users. All users, to include 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 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 users outside of the NRC that will have access to any PII.

To date, the NRC has approximately 20 representatives from the FBI who use 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 (WMD), critical infrastructure, and nuclear and radiological issues. All requests from the FBI for accounts in the PWS are reviewed and approved by the Office of Nuclear Security and Incident Response (NSIR) before being created. The NRC has the legal authority to share this information with the FBI under Section 221.b. of the Atomic Energy Act, codified at 42 USC 2271.

A Privacy Impact Assessment was performed by the agency for the system in August 2011. A SORN is not required for this system because it is not searchable by personally identifiable information. 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 on Personally Identifiable Information (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 staff estimates that 50 licensees will annually submit 339 reports through PWS, and that each report will require 2 hours to prepare and submit. The total licensee burden for this information collection is 678 hours at a cost of $184,416 (678 hours x $272/hr). 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 = 1000 hours per year @ $272/hr = $272,000
Contractual Support = $105,000 per year
TOTAL COST = $377,000

15. Reasons for Change in Burden or Cost

The NRC is submitting suspicious activity reporting using PWS as a request for a new clearance. PWS enables the NRC to fulfill its mission of communicating

sensitive information to licensees and developing more formal, long-term relationships with Federal, State, and local organizations with shared responsibilities for protecting nuclear facilities and activities and responding to incidents.

16. Publication for Statistical Use

    Due to the sensitivity of the information contained in PWS, all information is considered OFFICIAL USE ONLY and not to 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 (Voluntary)

Section	No. Of Respondents	Responses per Respondent	Total No. of Responses	Burden Hours per Response	Total Annual Reporting Burden (Hrs)
Voluntary Suspicious Incident Reporting	50	6.78	339	2	678
TOTAL	50		339		678

TOTAL BURDEN HOURS:	678 hours (678 hours reporting + 0 hours third party notification + 0 hours recordkeeping)
TOTAL BURDEN HOUR COST:	$187,716 (678 hrs x $272/hr)
ANNUAL RESPONDENTS:	50 respondents (none required)
RESPONSES:	339 responses (339 reporting responses + 0 third party responses + 0 recordkeepers)