UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF THE
INSPECTOR GENERAL

September 19, 2011

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

FROM: Stephen D. Dingbaum **/RA/**
Assistant Inspector General for Audits

SUBJECT: MEMORANDUM REPORT: AUDIT OF NRC'S SAPHIRE 8 SYSTEM (OIG-11-A-18)

OVERVIEW

The Office of the Inspector General (OIG) conducted an audit of the Nuclear Regulatory Commission's (NRC) SAPHIRE 8 System to determine if the system meets its required operational capabilities and applicable security controls. OIG determined SAPHIRE 8 meets its operational capabilities and there is limited security risk to the software. However, there are additional measures NRC should take to ensure SAPHIRE is managed properly. Specifically, OIG identified that formal policies and procedures on granting and managing access to SAPHIRE are needed. Furthermore, NRC identified the need for improvements to the SAPHIRE Web site user accounts and passwords.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this report. Actions taken or planned are subject to OIG followup as stated in Management Directive 6.1.

BACKGROUND

One of the NRC's key responsibilities is to help ensure that the operation of nuclear power plants and other NRC-licensed facilities presents no undue risk to public health and safety. The agency does this by applying and enforcing a set of technical requirements on plant design and operations. Since the 1970s, NRC has used

probabilistic risk assessment (PRA) as a tool for assessing, in a realistic manner, the strengths and weaknesses of nuclear plant design and operation. PRA is a technical analysis that systematically answers three questions: (1) What can go wrong? (2) How likely is it to happen? and (3) What are the consequences?

SAPHIRE Software Tool

NRC developed the Systems Analysis Programs for Hands-on Integrated Reliability Evaluations, or SAPHIRE, to aid in conducting these PRA evaluations. SAPHIRE is a software tool that performs the highly complex mathematics behind PRA. To use SAPHIRE, a user must first download a copy of the software to his or her personal computer.[1] The user must then input a detailed description of the systems, structures, and components (i.e., the model) to be analyzed in SAPHIRE. At NRC, these models, called Standardized Plant Analysis Risk (SPAR) models,[2] represent the as-built, as-operated nuclear plant. Once the SPAR model has been input, users can then enter different combinations of human and/or equipment failures and the nuclear plant's operating status (e.g., full power, low power, and shut down) to quantify the likelihood of an undesired end state, such as core damage. This allows NRC to model a nuclear power plant's response to accidents or potential events.

Other Federal agencies, some foreign government agencies, and members of the general public may also use SAPHIRE to conduct PRA evaluations on other complex systems, facilities, or processes outside the nuclear industry.

The initial version of SAPHIRE[3] was released in February 1987. The most current version of SAPHIRE, Version 8 (SAPHIRE 8), was released in April 2010. This version included more "user-friendly" features and new modeling and calculation methods, with the ability to handle larger and more complex PRA models than previous versions.

In addition to the downloadable SAPHIRE software tool, there is a secure SAPHIRE Web site (see figure, page 3). Access to the secure SAPHIRE Web site is restricted to approved users who are given unique personal identifications and passwords. Once users log into the Web site, they can access and download the most current version of

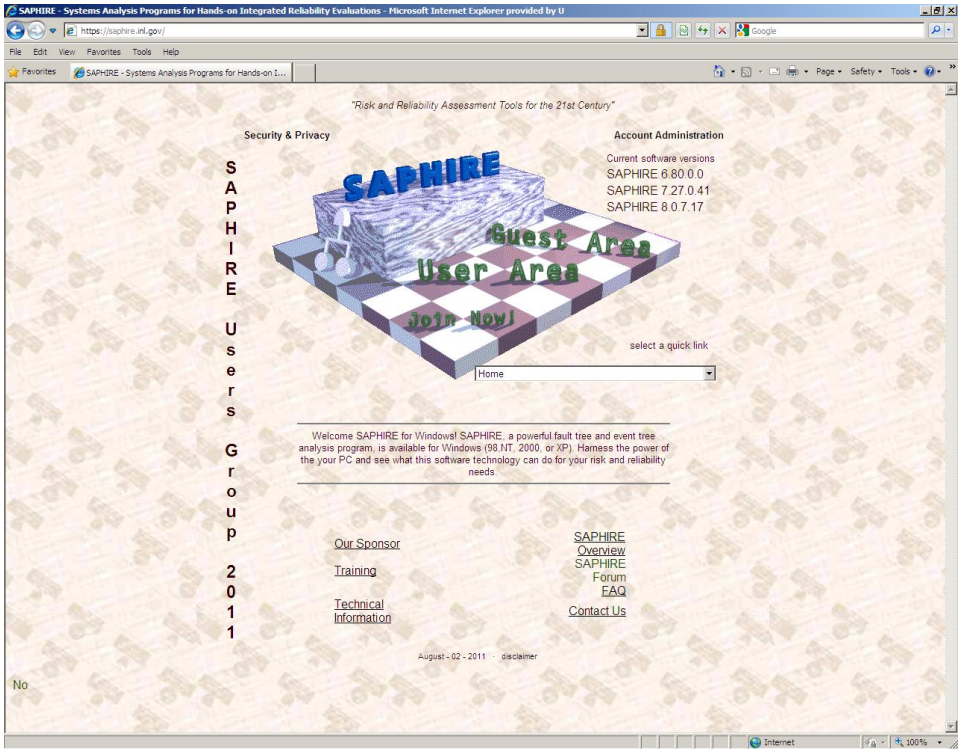
[1] Once the SAPHIRE software is downloaded to a user's personal computer, this software will reside on the user's machine permanently, unless deleted by the user.

[2] SPAR models are plant-specific PRA models that illustrate accident sequence progression, plant systems and components, and plant operator actions. The standardized models represent the as-built, as-operated plant. NRC staff use these SPAR models to independently assess the risk of events or degraded conditions at operating nuclear power plants.

[3] Initial versions of the PRA software tool were called the Integrated Risk and Reliability Analysis System. In 1997, the software name was changed to SAPHIRE.

the SAPHIRE software.[4] The Web site also allows users access to SAPHIRE guidance documentation and to submit questions or report any problems related to the software. A restricted section of the Web site allows only NRC users to access and download the most current version of the SPAR models.

Home Page of SAPHIRE Web site



Source: https://saphire.inl.gov/

SAPHIRE Users and Access

Access to the tool and Web site vary based on organization and user needs. The Office of Nuclear Regulatory Research (RES), the system owner of SAPHIRE, is responsible for granting user access to the software. Potential users must contact a specific individual in RES who handles all SAPHIRE access requests. For NRC employees, an e-mail request can be made directly to this individual, who then evaluates and determines the need for user access. If access is approved, NRC users are allowed access to the most current version of the software and full access to the Web site, including the SPAR models. While RES, the Office of Nuclear Reactor Regulation, and the Office of New Reactors all use SAPHIRE, the predominant users within NRC are the Senior Reactor Analysts located within each of NRC's four regional offices. The main Senior Reactor Analyst job function is to conduct PRA evaluations for issues and events related to the nuclear power plants in his or her region.

[4] Personal identifications and passwords are required only to access the SAPHIRE Web site. Once users have downloaded the SAPHIRE tool to their personal computers, the software can be used without a password. This also applies to SPAR models for NRC users.

While NRC users have unrestricted access to SAPHIRE 8 and the Web site, there are restricted access rights for non-NRC users. The ability to download SAPHIRE 8 is limited to NRC licensees, U.S. Government employees, their approved contractors, and some foreign government agencies.[5] Prior to access being granted, non-NRC entities typically[6] sign a non-disclosure agreement stating that users will not release the code to any third party without prior written consent from NRC. Once NRC reviews and approves these agreements, the entity's employees can then individually contact RES to request and download the SAPHIRE software. While non-NRC users who are granted access to the SAPHIRE Web site can access the SAPHIRE tool, they do not have access to the SPAR models.

Idaho National Laboratory (INL), the contractor[7] that developed SAPHIRE in conjunction with RES, also plays an important role in granting user access. While NRC is responsible for making determinations on who can have SAPHIRE, INL staff are responsible for providing the access to allow users to download the software. Additionally, INL generates SAPHIRE Web site user accounts for most users.[8]

Program Support Resources

INL interfaces with and supports SAPHIRE users. INL provides training courses to NRC staff and help desk support for NRC users. INL also provides support to the non-NRC user group. Furthermore, INL works closely with RES to resolve any outstanding issues, such as software bugs, user access, and overall continuous improvement of the system.

[5] Access to SAPHIRE 8 by some foreign government agencies is allowed. However, RES reviews these requests on a case-by-case basis.

[6] The only entity outside of NRC that is not required to sign a non-disclosure agreement is the National Aeronautics and Space Administration (NASA), the largest non-NRC user of SAPHIRE 8. In 2009, NRC signed a memorandum of understanding with NASA that established a collaborative agreement between the two agencies to share relevant technical information, reliability data, and software technology. With this agreement in place, NASA users are allowed access to SAPHIRE 8; therefore, signing a non-disclosure agreement prior to receiving access to SAPHIRE is not required.

[7] The Energy Reorganization Act of 1974 authorized the NRC to use the Department of Energy's (DOE) research facilities and services to assist NRC in conducting its mission. In 1978, NRC and DOE executed an MOU that established the policy governing the relationship between NRC and DOE for NRC-funded research at DOE laboratories. There are currently 17 DOE laboratories nationwide and all are managed and operated by non-Government entities under contract with DOE, including INL. In this report, "contract" refers to the agreement between NRC and the "contractor," DOE laboratory, INL.

[8] Based on the memorandum of understanding between NRC and NASA, NRC has delegated the responsibility for creating NASA user accounts to one NASA staff member. This person makes determinations concerning NASA employees' needs for access to SAPHIRE and the SAPHIRE Web site.

There are four ongoing SAPHIRE-related contracts, which have a total value of nearly $5 million. These contracts cover the time period of 2007 through 2013 and are specifically related to:

1. Coordination and integration of SPAR models.
2. Development of SAPHIRE 8.
3. Evaluating methods to improve SAPHIRE 8 speed and performance.
4. Maintenance and quality assurance activities related to SAPHIRE 8 code.

OBJECTIVE

The audit objective was to determine if the system meets its required operational capabilities and applicable security controls.

RESULTS

SAPHIRE 8 meets its operational capabilities and there is limited security risk to the software.[9] However, there are additional measures NRC should take to ensure SAPHIRE is managed properly. Specifically, OIG identified that formal policies and procedures on granting and managing access to SAPHIRE are needed. Furthermore, NRC identified the need for improvements to the SAPHIRE Web site user accounts and passwords.[10]

FINDING: FORMAL POLICIES AND PROCEDURES NEEDED

NRC lacks formal policies or procedures for granting and managing access to the SAPHIRE software. This occurs because agency managers have not prioritized the need for a formalized approach to managing access to SAPHIRE 8 and its Web site. As a result, more than half of the SAPHIRE Web site users have not accessed the site since July 2010. Without knowing the true universe of internal and external SAPHIRE users, NRC could have difficulty in managing user access.

Federal Guidance for Programs

Federal guidance states that Government programs, including information technology systems, should have formal guidance outlining proper policies and procedures. The National Institute of Standards and Technology (NIST) provides the Federal Government with guidance on security controls over information systems. A major component of system security is access controls. Access controls include (1) the

[9] SAPHIRE is listed by NRC's Office of Information Services as approved desktop software. SAPHIRE does not connect to any other NRC system and contains no sensitive information.

[10] The SAPHIRE Web site allows users to download the most current version of SAPHIRE. Additionally, NRC users can use the Web site to download the current SPAR models.

process of requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions. Specifically, NIST Special Publication 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations," states that when implementing an information technology system, there should be formally documented access control policies and a defined frequency for when these policies are reviewed and updated.

Informal User Access Policies and Procedures

NRC lacks formal policies or procedures for granting and managing access to the SAPHIRE software.

Granting User Access

When SAPHIRE 8 was initially developed, NRC staff discussed and determined who should be allowed access to the software. In November 2010, an e-mail documenting these decisions was circulated to the main NRC staff involved with managing and granting access to SAPHIRE. However, these decisions were never formally documented in official SAPHIRE policies, either for NRC or INL staff. The main INL contract staff person involved with granting user access was aware of the user access policy details, but could not locate any guidance materials describing this policy.

Reviewing User Access

There are no formal procedures to review user access to the SAPHIRE Web site on a regular basis. SAPHIRE Web site account holders have access to the Web site until they are removed from the approved user list. An NRC employee involved with SAPHIRE stated that he annually reviews the user list to determine if anyone no longer needs access due to separation from NRC or changed job responsibilities. If any accounts are identified as unneeded, the NRC employee will contact INL to have these accounts deleted. When this NRC employee took over responsibility for reviewing user access, his predecessor verbally informed him of this procedure; however, it was not documented. Furthermore, the NASA staff member responsible for granting all NASA users access to SAPHIRE 8 does not review the universe of Web site users. He stated that there are a small number of users and he is able to see who has access, but he does not perform any checks to determine if users still need access. This NASA employee said that removing access from those who no longer need access is an area that needs improvement.

Not Viewed As a Priority

There are no formal policies and procedures because agency managers have not prioritized the need for a formalized approach to managing access to SAPHIRE 8 and its Web site.

Granting User Access

A senior NRC manager stated that formally documenting policies and procedures on who is allowed access to SAPHIRE 8 and the Web site has not been viewed as a priority since there are a small number of people involved with managing SAPHIRE.

Reviewing User Access

NRC managers have not taken a formal approach to reviewing needed user access because they have not perceived this as necessary. The NRC staff member involved with reviewing access stated that the number of users who have access to SAPHIRE is small; therefore, he is familiar with who no longer needs access. While INL is able to produce SAPHIRE user logs showing the last time approved users accessed the Web site, NRC has not requested these logs to help determine who still needs access during its annual review of user accounts.

Furthermore, NRC staff stated that maintaining a user account after it was no longer needed would not result in potential access to sensitive information. In a December 2007 report, "Sensitive Unclassified Non-Safeguards Information (SUNSI) Assessment of SAPHIRE and SPAR Models," NRC reviewed the sensitivity of the software and the related models, which composes the information available on the SAPHIRE Web site. This report concluded that unauthorized access to SAPHIRE or SPAR models does not pose a threat to any sensitive information.

Too Many Users Have Access

Because the agency lacks a formal approach to updating SAPHIRE Web site access lists, more than half of the approved users have not accessed the Web site since July 2010. Many said while they once had a need for SAPHIRE, this is no longer the case. Without knowing the true universe of users, it is difficult for NRC to manage user access.

OIG performed an analysis to determine the total number of users and their level of involvement with the SAPHIRE Web site. INL provided reports that detailed the total users broken down by organization, and the total number of Web site log-ins per user from August 2010 through June 2011. Using this information, OIG determined that more than 50 percent of the total user population had not logged into the SAPHIRE Web site since July 2010 or earlier. The following table provides a breakdown of the main user groups and the percentage of inactive accounts.[11]

[11] Inactive accounts are SAPHIRE Web site accounts with no log-ins occurring since at least August 2010.

Inactive SAPHIRE Accounts as of June 2011

	Number of User Accounts	Inactive Accounts	Percentage of Accounts Inactive
NRC	194	102	53%
NASA	71	55	77%
INL	37	16	43%
Other	11	5	45%
Total	**313**	**178**	**57%**

Source: OIG analysis of Web site usage data.

OIG interviewed a judgmental (non-statistical) sample of approximately 20 percent of the inactive NRC user account holders. Of these 21 inactive users, 13 stated that they would no longer need access to the SAPHIRE Web site. Seven of the thirteen stated that they had not accessed the SAPHIRE Web site in several years. One inactive user claimed that he had not accessed the SAPHIRE Web site in approximately 10 years. However, some of the inactive user account holders expect to need access in the future. For example, one account holder remarked that while he has not used SAPHIRE to this point, using the software will soon become part of his job responsibilities.

Without knowing the true universe of users, it is difficult for NRC to manage access to the program consistent with NIST guidance on access controls. Although OIG did not discover any instances of inappropriate access being granted to the software tool, many users have maintained Web site access after it was no longer needed. Documented policies and procedures for managing user access could significantly increase the security controls over the system. Furthermore, formal written documentation on granting and managing access to SAPHIRE 8 would assist any new staff who become involved with SAPHIRE management.

Recommendations

OIG recommends that the Executive Director for Operations:

1. Formalize a policy on granting access to SAPHIRE 8.

2. Develop and implement SAPHIRE Web site procedures to:

   - Check and verify continued need for user access.
   - Deactivate unnecessary user accounts.

3. Develop and implement an automated system to deactivate SAPHIRE Web site user accounts that have not been used in a defined time period (e.g., 6 months).

OBSERVATION: IMPROVED USER ACCOUNT SECURITY NEEDED

At the initiation of this audit, NRC identified the need for improvements to the SAPHIRE Web site user accounts and passwords. Currently, all SAPHIRE Web site user accounts are created by two individuals:

1. An INL contractor, who creates the majority of user accounts/all non-NASA accounts.

2. A NASA employee, who creates only the NASA employee and NASA contractor accounts.

When the user account is created, the individual who generated the account determines a password to be assigned to this account. This password never expires and is never required to be changed. While both the INL contractor and the NASA employee stated that the user account passwords they have created recently are complex in nature, some of the older accounts may not meet any complexity standards.

NRC is currently working to improve the process for generating user accounts and passwords. Specifically, a modification to the SAPHIRE contract that focuses on improving SAPHIRE Web site security was developed in July 2011. Currently, RES is working through the administrative process to formally include this modification as a contract requirement. This modification requires INL to develop and implement a plan to improve the security controls applied to SAPHIRE Web site user accounts. The plan,

which will require NRC approval before implementation, will likely include changes to the user accounts to have passwords that:

- Are generated by the individual users.
- Have expiration dates.
- Meet certain complexity standards.

OIG contends that this contract modification will improve the security of the SAPHIRE Web site and advises that NRC continue to pursue these improvements to SAPHIRE Web site user accounts and passwords.

AGENCY COMMENTS

An exit conference was held with the agency on September 13, 2011. At this meeting, agency management provided supplemental information that has been incorporated into this report as appropriate. As a result, agency management stated their general agreement with the findings and recommendations in this report and opted not to provide formal comments for inclusion in this report.

SCOPE AND METHODOLOGY

OIG audited SAPHIRE 8 to determine if it meets its required operational capabilities and applicable security controls. The audit team reviewed relevant criteria, including NIST Special Publication 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations"; FIPS Publication 200, "Minimum Security Requirements for Federal Information and Information Systems"; NUREG 1925 "Research Activities FY 2010 – FY 2011"; "Sensitive Unclassified Non-Safeguards Information (SUNSI) Assessment of SAPHIRE and SPAR Models"; and the Government Accountability Office's "Standards for Internal Control in the Federal Government." OIG auditors also reviewed previous NRC OIG audit reports including, "Evaluation of NRC's Use of Probabilistic Risk Assessment (PRA) in Regulating the Commercial Nuclear Power Industry" (OIG-06-A-24).

At NRC headquarters, in Rockville, MD, auditors interviewed RES, Office of Nuclear Reactor Regulation, and Office of New Reactors staff and management to gain an understanding of their roles and responsibilities related to SAPHIRE 8. Auditors conducted telephone interviews with NRC regional staff and management, as well as staff from INL and NASA. Additionally, OIG attended 1 day of a 3-day PRA training class conducted by INL at NRC's Professional Development Center in Bethesda, MD.

We conducted this performance audit at NRC headquarters from May 2011 to July 2011 in accordance with generally accepted Government auditing standards. Those standards require that the audit is planned and performed with the objective of obtaining sufficient, appropriate evidence to provide a reasonable basis for any findings and conclusions based on the stated audit objective. OIG believes that the evidence obtained provides a reasonable basis for the report findings and conclusions based on the audit objective. Internal controls related to the audit objective were reviewed and analyzed. Throughout the audit, auditors were aware of the possibility or existence of fraud, waste, or misuse in the program. The work was conducted by Beth Serepca, Team Leader; Rebecca Underhill, Audit Manager; Yvette Mabry, Senior Auditor; and Michael Blair, Management Analyst.

CC: N. Mamish, OEDO
J. Arildsen, OEDO
K. Brock, OEDO
C. Jaegers, OEDO

Electronic Distribution

Edwin M. Hackett, Executive Director, Advisory Committee
on Reactor Safeguards
E. Roy Hawkens, Chief Administrative Judge, Atomic Safety
and Licensing Board Panel
Stephen G. Burns, General Counsel
Brooke D. Poole, Director, Office of Commission Appellate Adjudication
James E. Dyer, Chief Financial Officer
Margaret M. Doane, Director, Office of International Programs
Rebecca L. Schmidt, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
R. William Borchardt, Executive Director for Operations
Michael F. Weber, Deputy Executive Director for Materials, Waste,
Research, State, Tribal, and Compliance Programs, OEDO
Darren B. Ash, Deputy Executive Director
for Corporate Management, OEDO
Martin J. Virgilio, Deputy Executive Director for Reactor
and Preparedness Programs, OEDO
Nader Mamish, Assistant for Operations, OEDO
Kathryn O. Greene, Director, Office of Administration
Patrick D. Howard, Director, Computer Security Office
Roy P. Zimmerman, Director, Office of Enforcement
Cynthia Carpenter, Acting Director, Office of Federal and State Materials
and Environmental Management Programs
Cheryl L. McCrary, Director, Office of Investigations
Thomas M. Boyce, Director, Office of Information Services
Miriam L. Cohen, Director, Office of Human Resources
Michael R. Johnson, Director, Office of New Reactors
Catherine Haney, Director, Office of Nuclear Material Safety
and Safeguards
Eric J. Leeds, Director, Office of Nuclear Reactor Regulation
Brian W. Sheron, Director, Office of Nuclear Regulatory Research
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
James T. Wiggins, Director, Office of Nuclear Security
and Incident Response
William M. Dean, Regional Administrator, Region I
Victor M. McCree, Regional Administrator, Region II
Mark A. Satorius, Regional Administrator, Region III
Elmo E. Collins, Jr., Regional Administrator, Region IV