

NEESComm Cybersecurity Plan

Saurabh Bagchi, Rudolf Eigenmann, Dawn Weisman, Thomas Hacker

NEEScomm IT Team

1 Introduction

The NEES Cyberinfrastructure (CI) system is composed of fourteen equipment sites and one central IT facility, henceforth referred to as NEEScomm IT. With IT resources (hardware and software) spread across the system and connected together with internet protocols over the public internet, computer security is of prime concern. As a leading Cyberinfrastructure project, NEES has developed a comprehensive cybersecurity approach that includes best practice cybersecurity policies and mechanisms at NEESCentral and an annual security audit at each of the NEES sites.

The purpose of the NEEScomm CyberSecurity Plan (CSP) is to:

- Delineate responsibilities, roles and expected behavior of all individuals who access NEEScomm IT services.
- Provide an overview of the security requirements for NEES machines at the sites.
- Identify a strategy for responding to security incidents.

The security plan should be viewed as documentation describing the structured process to plan adequate, cost-effective security protection for NEES CI. As a result, this document provides a list of standards, guidelines and procedures for the implementation of the NEEScomm CSP. It is recommended that the security plan be reviewed and updated annually to reflect enhancements to the NEEScomm IT services, the assets at the sites, and to react to new security threats from the ever-changing computer security field.

The target audience for this document is for the entire NEES community. This audience includes NEES IT members at NEES headquarters, NEES IT members at each site, and researchers and practitioners in earthquake engineering who make decisions involving or make use of NEES information technology systems.

The current document builds on several sources, including the last available NEES cybersecurity policy document [2]. However, the document is outdated (it dates back to 2005). Much of the policy was never put in practice and many of the IT resources and practices have changed since then. This current document is therefore significantly different from this previous document.

2 Roles and Responsibilities

NEES CI security is the responsibility of everyone who can affect the security of NEES CI systems. However, since the specific duties and responsibilities of various individuals and organizational entities vary considerably, certain key responsibilities should be made explicit for the sake of clear accountability.

2.1 Senior Management

Ultimately, overall responsibility for the success of the NEES CI system lies with the senior management team comprising the NEES IT Director, the NEES IT Leader, and the NEEScomm Center Director at NEEScomm IT. This management team will be assisted by the NEEScomm Cybersecurity Officer (CSO) in the matter of the cybersecurity program and its overall goals, objectives, and priorities in order to support the overall mission of NEES. The senior management team is also responsible for ensuring that adequate resources are applied to the security program to ensure its success.

2.2 Cyberinfrastructure Security Management

The NEES CSO (currently identified as Saurabh Bagchi at NEEScomm) in collaboration with the NEES IT director directs NEEScomm's day-to-day management of its security program, including maintaining a security website with policies and guidelines, providing security advice to the NEES community, and conducting regular security audits. This person is also responsible for coordinating all security related interactions among the various participating organizations of NEES.

2.3 Site IT Managers

To ensure that proper security measures are taken at each equipment site, site security should ultimately be the responsibility of both the NEES equipment site Principal Investigator and the Site IT Managers (SIMs) who are responsible for the day-to-day operations of the NEES equipment sites, including the supporting computer systems. Their responsibilities include enforcing appropriate security controls such as management, operational, and technical controls that comply with NEEScomm's CSP. It is the SIMs who are ultimately responsible for the security of a site's IT systems. They are responsible for implementing technical security on computer systems and for being familiar with security technology that relates to their systems. They also are required to ensure the continued operation of their IT services to meet the needs of NEES researchers, as well as analyze technical vulnerabilities in their systems and their security implications.

3 Authentication and Authorization Policy

Controlled access to IT resources is essential for NEEScomm to fulfill its mission. This policy describes our plan for Authentication and Authorization that can support current needs for electronic access and

accommodate future services and technologies by employing standardized mechanisms for Identification, Authentication, and Authorization.

3.1 Objective

This policy is guided by the following objectives:

1. To ensure that NEEScomm can, without limitation, operate and maintain its IT resources;
2. To ensure that NEEScomm can, without limitation, protect the security and functionality of its IT resources and the data stored on those resources;
3. To protect NEEScomm's other property, rights, and resources;
4. To preserve the integrity and reputation of NEEScomm;
5. To safeguard the privacy, property, rights, and data of users of NEEScomm IT;
6. To comply with applicable existing NSF regulations; and
7. To comply with existing Purdue University¹ policies [1], standards, guidelines, and procedures.

3.2 Policy Statement

Access Control

Identification, Authentication, and Authorization are controls that facilitate access to and protect NEEScomm IT resources and data. Access to non-public IT resources will be achieved by unique User Credentials and will require Authentication.

NEEScomm will assign a username and password for Identification and Authentication purposes to each individual that has a business, research, or educational need to access NEEScomm IT resources. In all cases, only the minimum privileges necessary to complete required tasks are assigned to that individual. Privileges assigned to each individual will be reviewed on a periodic basis and modified or revoked upon a change in status within the NEES community.

A user at a site² will be given privileges upon the submission of an account request form (available from <https://www.nees.org/it/support/security/>) by the individual. The request form should bear the approval of the SIM and the site operations manager from the individual's site. Also, upon the expiry of the work need of the individual, the SIM should promptly notify the NEEScomm CSO. The assignment of user account for individuals not at a site will be decided based on an application from the individual. Different

¹ Henceforth, whenever just University is mentioned without any qualification, it will mean Purdue University.

² The term "user at a site" comprises all researchers at an earthquake engineering site that use NEEScomm IT resources. This would include the NEESR PI, her students, the site operations manager, and the site IT manager.

levels of user accounts, with different privileges, may be assigned depending on the nature of access required. The CSO is responsible for making the decision in consultation with the senior management.

All NEEScomm IT resources must use only encrypted Authentication and Authorization mechanisms unless otherwise authorized by the CSO.

User Credentials Standard

The password will be used as the primary user credential, to be used along with the username. A password may be used only by the authorized user. Passwords or accounts should never be shared with anyone, including trusted friends or family members. Account owners will be held responsible for any actions performed using their accounts. NEES IT staff will never ask users to disclose their passwords in any manner. Passwords should never be written down and left in plain sight, or stored in plain text online.

Passwords for NEEScomm IT resources must comply with the following standards:

- Passwords must contain at least 1 letter.
- Passwords must contain at least 1 number or punctuation mark.
- Passwords must be at least 8 characters long.
- Passwords must contain more than 4 unique characters.
- Passwords must not contain easily guessed words (e.g. Purdue, nees, boiler).
- Passwords must not contain your name or your username.
- New passwords must be different than the previous password (re-use of the same password will not be allowed for one (1) year).

The use of group accounts for administrative purposes and shared passwords for those accounts should be minimized where technically feasible. In situations where group accounts for administrative purposes and shared passwords for those accounts is required (e.g. “Root” or “Administrator” accounts), the passwords used must also follow the standards stated above.

Password Expiration

All NEEScomm IT resource passwords must be changed at least every one hundred twenty (120) days. Any group password must be changed every one hundred twenty (120) days and immediately upon any personnel change within the group

Two-Factor Authentication

Two-factor authentication (TFA) offers inherently greater security than reusable passwords. TFA utilizes a “something you have and something you know” method of authenticating users. The “something you

have” is a hardware device such as a token or smart card, and the “something you know” is a PIN (personal identification number, or alphanumeric code). The combination of the hardware device and the PIN authenticates users to systems. NEEScomm IT will be using RSA SecurID fobs selectively for controlling access to critical IT assets. What constitutes critical IT assets is an operational decision that will be made by the NEEScomm IT Director and the CSO as and when the situational need arises. When a user is given such a fob, the following pin requirements for TFA will hold:

- It must be at least 4 characters long.
- A PIN should avoid easily guessed sequences such as “1234” or “abcd.”
- If the PIN is numeric, it should not contain information identifying the user such as Social Security Number (SSN), PUID, or other information publicly obtainable about the user.
- If the PIN is alphanumeric, it should contain both characters and numbers.
- If alphanumeric, a PIN should not contain easily guessed words.
- If alphanumeric, a PIN should not contain the user’s name or parts of the name, or information publicly obtainable about the user (e.g., address, phone number, office number)
- A changed PIN should be substantially different from the previous PIN.
- A PIN should be memorized.
- A PIN should not be reused within one year.

In addition, TFA devices of all kinds (tokens, smart cards, etc.) should be safeguarded and kept with the user at all times. If the TFA device has been lost or stolen, this should be reported to the NEEScomm CSO immediately. There is currently no requirement to change the PIN on a TFA device. However, the longer a PIN remains unchanged, the greater the risk of certain types of attacks. The CSO recommends that PINs be changed at least yearly.

4 Privacy Policy

The right to privacy is a deeply held conviction, especially within intellectual and academic communities. Privacy is critical to the intellectual freedom that forms the foundation of higher education. While the right to individual privacy is highly valued in the University community, it must, however, be balanced with legal obligations and the larger needs of the community.

Although NEEScomm seeks to create, maintain, and protect the privacy of electronic information on its IT resources, users should be aware that the use of NEEScomm IT resources is not completely private. Accordingly, users of NEEScomm IT resources are hereby specifically notified that they have no expectation of privacy in connection with their use of such IT resources. Except as provided in this

policy, NEEScomm does not routinely monitor the content of communications or transmissions using IT resources. The normal operation and maintenance of the NEEScomm IT resources require the back up and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities. There are also special circumstances such as illness; death; violation of NEEScomm policies, regulations procedures or rules; or illegal activity which may warrant intrusive or restrictive action within an individual's computer account and/or devices.

4.1 Objective

The purpose of this policy is to outline the special circumstances under which NEEScomm may access content or electronically stored wire and electronic communications and information on its IT resources in order to protect its legitimate operational and strategic interests. Those interests include NEEScomm's need to ensure that it can, without limitation, operate and maintain its IT resources as well as protect the integrity, security, or functionality of data stored on NEEScomm IT; protect NEEScomm's other property, rights, and resources; ensure compliance with University policies, procedures, or regulations; preserve the integrity and reputation of the University; safeguard the property, rights, and data of third parties; and comply with applicable laws.

4.2 Policy Statement

This policy covers the following types of information:

1. Data and computer accounts on NEEScomm systems or other NEEScomm-owned devices.
2. Voice and data telecommunications traffic to, from, or between IT resources, including without limitation any of the devices listed above.

In general, the types of information enumerated above are considered private and cannot be accessed by someone other than the person to whom the IT resource account has been assigned, the person from whom the information originated, or the person to whom the device has been assigned. According to the separate data sharing and archiving policy, project data must be uploaded to NEEScomm Data Repository and made public after a certain length of time. Furthermore, as noted above, NEEScomm does not routinely monitor the content of communications or transmissions using IT resources. NEEScomm does, however, specifically reserve the right, with or without notice, to intercept, access, monitor, inspect, copy, store, use, or disclose the contents of communications or transmissions employing IT resources when it reasonably believes these actions are appropriate in order to protect its interests.

More specifically, and without limiting the foregoing general rights, NEEScomm reserves the right to monitor and inspect computer accounts and devices as warranted by the need to protect the information and services held on NEEScomm IT resources and any legal obligations that arise, and NEEScomm may,

without notice, use: (a) security tools designed to locate security flaws in equipment connected to IT resources; (b) network monitoring hardware and software that capture the contents of packets traversing the network; (c) network hardware and software designed to protect IT resources and users of IT resources, including without limitation Anti-Phishing Services, Anti-Virus Services, Intrusion Detection Systems, Spam Filtering Services, and Anti-Spyware Services; or (d) system log information, including without limitation source and destination for a connection, session start and end times, login name, timestamps, and commands issued. In addition, and again without limiting the above-enumerated general right to act when it reasonably believes these actions are appropriate in order to protect its interests, NEEScomm may, acting through NEEScomm-authorized technicians and administrators and pursuant to the procedures specified herein, access or permit access to the contents of communications or electronically stored wire and electronic communications and information employing IT resources if it:

- Has a reasonable belief that a process active in the account or device is causing or may cause significant damage to NEEScomm IT resources or could cause loss/damage to user, NEEScomm, or third-party data.
- Receives a written request from federal, state, or local law enforcement agencies and complies with applicable NEEScomm policies.
- Has a reasonable belief that an individual has or is violating NEEScomm policies, regulations, procedures, or rules using the accounts or devices in question.
- Receives a written request from the NSF Director of Audits when an audit is investigating fiscal misconduct linked to the user whose account or device is in question.
- Is authorized by an appropriate order of a court of competent jurisdiction and complies with applicable NEEScomm policies relating to the handling of such orders.

Again, without limiting the foregoing general rights, NEEScomm may, in its sole discretion, disclose the results of any general or individual monitoring or accessing permitted as described below in this section, including the contents and records of individual communications, to appropriate NEEScomm personnel or law enforcement agencies or use those results in appropriate NEEScomm disciplinary proceedings. Where applicable and warranted, the account or equipment user will be notified of the accessing or monitoring and the corrective actions taken.

The contents of the user's e-mail, computer accounts, devices, and network traffic may be recorded and stored to prevent destruction should the information be requested pursuant to valid legal process.

The NEEScomm Center Director or his or her designee may authorize access in the event that he or she reasonably determines that: (a) there exists an emergency that materially threatens NEEScomm's interests, (b) that emergency access is reasonably required in order to protect the NEEScomm's interests, and (c) he

or she specifies the scope and conditions of any permitted access. The CSO shall, as soon as reasonably possible after such emergency, make a written finding verifying the existence and satisfaction of the foregoing conditions.

Any access permitted hereunder shall be the minimum access required in order to protect NEEScomm's interests.

5 Incident Response Policy

For the purpose of this section, we define an incident as any event involving NEEScomm IT resources which:

- violates local, state or U.S. federal law, or
- violates regulatory requirements which NEEScomm is obligated to honor, including without limitation regulatory requirements specified by NSF, or
- violates a Purdue University policy, or
- is determined to be harmful to the security and privacy of NEEScomm data, or IT resources, or
- constitutes harassment under applicable law or University policy, or
- involves the unexpected disruption of NEEScomm services.

The responsibility for responding to an incident lies with the Coordinator of Incident Response, or CIR. The NEEScomm CSO currently fulfills the role of CIR.

5.1 Objective

A formal policy for the reporting of and response to IT incidents is necessary to ensure the secure operation of NEEScomm IT resources, to protect the data security and privacy of all NEEScomm users. This section sets forth a set of policies for any NEEScomm user to report any incident to the NEEScomm CIR and for the efficient response to IT incidents in order to maintain the security and privacy of IT resources, data and other assets, as well as satisfy requirements of state and federal law.

5.2 Policy Statement

Reporting an incident

NEEScomm users should report any incident, even if they are not completely certain if it falls under the purview of the definition of incident given above, to the NEEScomm IT team at the earliest possible opportunity. The effect of the incident may be restricted to the site's IT resource as it pertains to the operation of NEEScomm or it may apply to the NEEScomm IT resources at Purdue University. Examples of incidents which need to be reported are breakin to a legitimate user account, data being compromised

because it lay unprotected for some length of time, detection of malicious scans originating from a site, and evidence of malware infecting machines at the sites which are used to access NEEScomm IT services. To report an incident, the user is expected to abide by the following guidelines:

1. If the incident is likely restricted to the site's IT resources only, then the user should use the web form at <https://www.nees.org/it/support/security/> to report the incident. The web form will guide the user to provide as much of the relevant details as possible, including, but not limited to, the hardware and the software configuration of the machines affected by the incident, the time of the first observation of the incident and the ingress point, and the extent of the effect on the site's IT resources. The web form will ask the user to submit a contact telephone number so that the CIR can contact the user for remediation actions. The user should use a machine that is definitely not affected by the incident for this said reporting purpose. On receiving the report, a NEEScomm staff will immediately acknowledge receipt and the CIR will generate the initial response within 8 hours. If the acknowledgment of receipt is not received by the user, then he/she should use option 2 immediately since it indicates the reporting of the incident was not successful.
2. For broader scopes of the incident than in item 1 above, the user should use the toll-free number for NEEScomm IT purposes. On dialing this toll-free number, the user will be directed to an option for reporting cybersecurity incidents. This number will be staffed 24x7 and the CIR will provide an initial response within 8 hours of the incident report filed through the telephone call.

Receiving Reports

The CIR upon receiving a report is responsible for assessing its veracity, determining whether or not the event constitutes an IT incident and classifying the IT incident, and initiating handling procedures. The CIR reserves the right, subject to applicable law and other applicable NEEScomm policies, to use the following resources for IT incident detection and/or response:

1. System and application logs
2. Passive network traffic monitoring (e.g., IDS, and other network packet analyzers)
3. Active scanning of systems suspected of violating NEEScomm policy, or systems exhibiting symptoms of compromise
4. Other resources as determined appropriate by the CIR and as allowed by NEEScomm policy and applicable law.

To facilitate accurate reporting, handling, and record keeping, the above two-step process should be followed for communicating an incident report. The CIR should also maintain a record of communication and data collection for all events reported to the CIR.

Classification

In order to facilitate the accurate and productive response to IT incidents, all IT incidents must be classified and assessed by the CIR for severity at their onset. As the IT incident progresses, its classification may be reevaluated and changed as necessary to ensure proper handling. We will follow the classification system outlined below for NEEScomm IT incidents.

Rating	Definition
Critical	A vulnerability whose exploitation could damage NEEScomm IT services, without user action.
Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users data, or of the integrity or availability of processing resources.
Moderate	Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.
Low	A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

In some cases, IT incidents may fall under multiple classifications. When this happens, the classification with the highest severity should generally dictate the course of IT incident response. The CIR is responsible for providing and maintaining appropriate IT incident classification guidelines and resolution procedures.

Any incident which is of important or higher rating will be reported to NSF. NSF may impose further reporting requirements for security incidents, at its discretion.

Response

After receiving a report, assessing its veracity, determining whether or not the event constitutes an IT incident, and classifying the IT incident, the CIR will determine if the IT incident warrants a formal response. IT incidents that do not warrant formal response at the NEEScomm IT level will be remanded to the appropriate SIM for handling. All reported events or IT incident must be documented throughout the response process.

If an event report does warrant formal IT incident response procedures by the CIR, it is the responsibility of the CIR to coordinate the appropriate resources for such response. If deemed appropriate by the CIR, a team of NEEScomm IT staff will be formed and led by the CIR for responding to the IT

incident. The CIR is responsible for documenting appropriate procedures for responding to event reports and IT incidents, and coordinating incident response teams.

Business Continuity

In the course of responding to an IT incident it may be necessary, subject to applicable laws and NEEScomm policies, to require the suspension of involved or targeted services/systems in order to:

- Protect NEEScomm users, IT resources, other systems, data, and University assets from threats posed by the involved services/systems
- Protect the service/system in question
- To preserve evidence and facilitate the IT incident response process

The decision to suspend operations will be made by the CIR, and will require approval by the NEEScomm IT Director and the NEEScomm Center Director. In the case of mission critical applications, the CIR will make a good-faith effort to consult with the appropriate SIM, and if available, service/application owner before such suspensions are carried out. If, in the judgment of the CIR an excessive amount of time (giving due weight to the relative severity of the IT incident) has passed without response from the appropriate SIM or service/application owner, suspension may occur without consultation.

Any equipment not owned by a valid NEEScomm user which is using NEEScomm IT resources, and is found to be the target, source, or party to an IT incident may be subject to immediate suspension of services without notice until the issue has been resolved, or the subject system is no longer a threat.

In all cases, it is the CIR who shall determine if and when a service suspension may be lifted.

In order to facilitate proper and timely handling of IT incident responses, it is necessary that network-connected devices can be identified and located as soon as possible. To this end, SIMs are required to maintain an inventory of network-connectable devices under their control that are used to access NESScentral resources. This inventory should include, at a minimum, the primary location of the device, and the addresses for all network interfaces used by the device (per machine MAC address and all IP addresses for a machine).

6 Site Audit Policy

NEEScomm's comprehensive cybersecurity approach includes a security audit at each of the NEES sites performed once a year. The audits use security best practices to verify that each server-class system operating at a NEES site is operating in a manner to limit the potential for security incidents and breaches. Such events could invalidate data being collected by scientists, damage experimental equipment, and

spread the damage to the NEEScomm IT resources. No system can be perfectly secure, to be sure. But regular audits of the system provide vital information for the regular upkeep and secure maintenance of the server systems. This section outlines the policies that will govern the audits of the site resources.

6.1 Objective

The objective of this policy section is to enable security audits with minimal impedance to the activities at each site and making the best possible use of the time and resources of IT personnel at the sites and at NEEScomm. It also lays out certain minimal requirements for the security audit as well as preferred practices that go above and beyond the minimal requirements. Yet another objective is to lay out the goals and the expected follow-on activities from a security audit.

6.2 Policy Statement

Schedule for the audit scans

Each SIM together with the NEEScomm CSO, or his designee, will work together to determine an appropriate time schedule for performing the audit. The audits will generally be done once a year. However, in the event that a security incident is suspected to have occurred or is anticipated, say due to the release of a dangerous malware that affects the IT systems at one or more sites, then further audits will be done. In all cases, the timing for the audit will be decided in consultation with the SIMs, such that the site operations are minimally affected and the resources of the site IT staff are optimally utilized.

Running the audit scans

The set of scan software that will be a part of the audit will be provided by NEEScomm. It is known that some of the scan software used in the previous audit are no longer being maintained and therefore do not serve the purpose of a security audit. These will be replaced by a new set of audit software.

It is desirable that the audits be done in a manner that is as automated as possible. For this NEEScomm will generate, as far as practicable, scripts to run the audit scans automatically, collect the results, and perform a first-pass automated analysis of the scan results to identify any security vulnerabilities. The scan must originate from a machine within the university that the site is a part of. It is expected that for such technical reasons as well as operational reasons, the execution of the audit scans will be done with the participation of the SIM. The parties will determine which machines will be a part of the scan. This will be derived from the inventory of the site IT assets that will be done at the beginning of each project year. All the IT assets that are related to NEES activities, including, but not restricted to the following will be a part of the security audit – local data repositories, and machines operated by the NEES network and used to access NEEScomm IT data and NEEScomm IT services.

Actions following the audit scans

Upon completion of the audit scans, the automation script will parse the results of the scan and from it identify any vulnerabilities that the scans uncovered. Any such discovered vulnerability will initiate an incident report and will follow the steps outlined above in Section 5. The automated analysis will be executed promptly upon completion of each audit scan. Note that the entire audit will consist of multiple scans, each using a different software package.

Upon completion of the automated analysis of the scan reports, a more detailed and manual analysis of the report will be done by the NEEScomm security staff. The objective of this is to identify vulnerabilities that are very difficult to be covered by any automated analysis script due to the evolving nature of the computer security threats. If this manual analysis finds any vulnerability or evidence of a security breach, the SIM will be immediately contacted and an incident report initiated.

A formal report will be generated once a year that summarizes the results of the audits for each site. The report will identify the assets that were a part of the audit, where the audit did find vulnerabilities and security breaches, and remediation actions, both short term and long term. This report will not be for public disclosure, keeping in view the security sensitive nature of the information. The report will be seen only by NEEScomm members, site IT members, and NSF.

Low intensity periodic scans

In addition to the annual audits, NEEScomm will install scan software that can do periodic low intensity audit scans. Such software will be from reputable sources (often from the same sources that provide the software for the annual audits). The goal of these periodic scans is to identify vulnerabilities as they come up and any possible security breaches, closer to the time of occurrence of the breach than would be possible through the annual audits. For these periodic scans, it is again important that the site activities be minimally affected, if at all. Therefore, the schedules for these scans and their priority levels will be decided by the NEEScomm CSO in consultation with the SIMs.

7 Conclusion

In this document, we have outlined the NEES Cyberinfrastructure (NEES CI) security plan that delineates the responsibilities, roles, and expected behavior of all individuals who access NEEScomm IT services and the policies governing the security controls that will be used to minimize the risks of cybersecurity incidents. All site IT personnel and NEEScomm IT staff should become familiar with this document. The security plan will be reviewed and updated annually to reflect enhancements to the NEEScomm IT services and to react to new security threats from the ever-changing computer security field.

References

1. Purdue University, "IT Policies Hierarchy", At:
<http://www.purdue.edu/securepurdue/bestPractices/policiesHierarchy.cfm>. Retrieved on October 23, 2009.
2. NEESIt, "NEES Cyberinfrastructure Security Plan," At:
https://www.nees.org/images/pdf_documents/neesit_sec-plan.pdf. Retrieved on October 23, 2009.