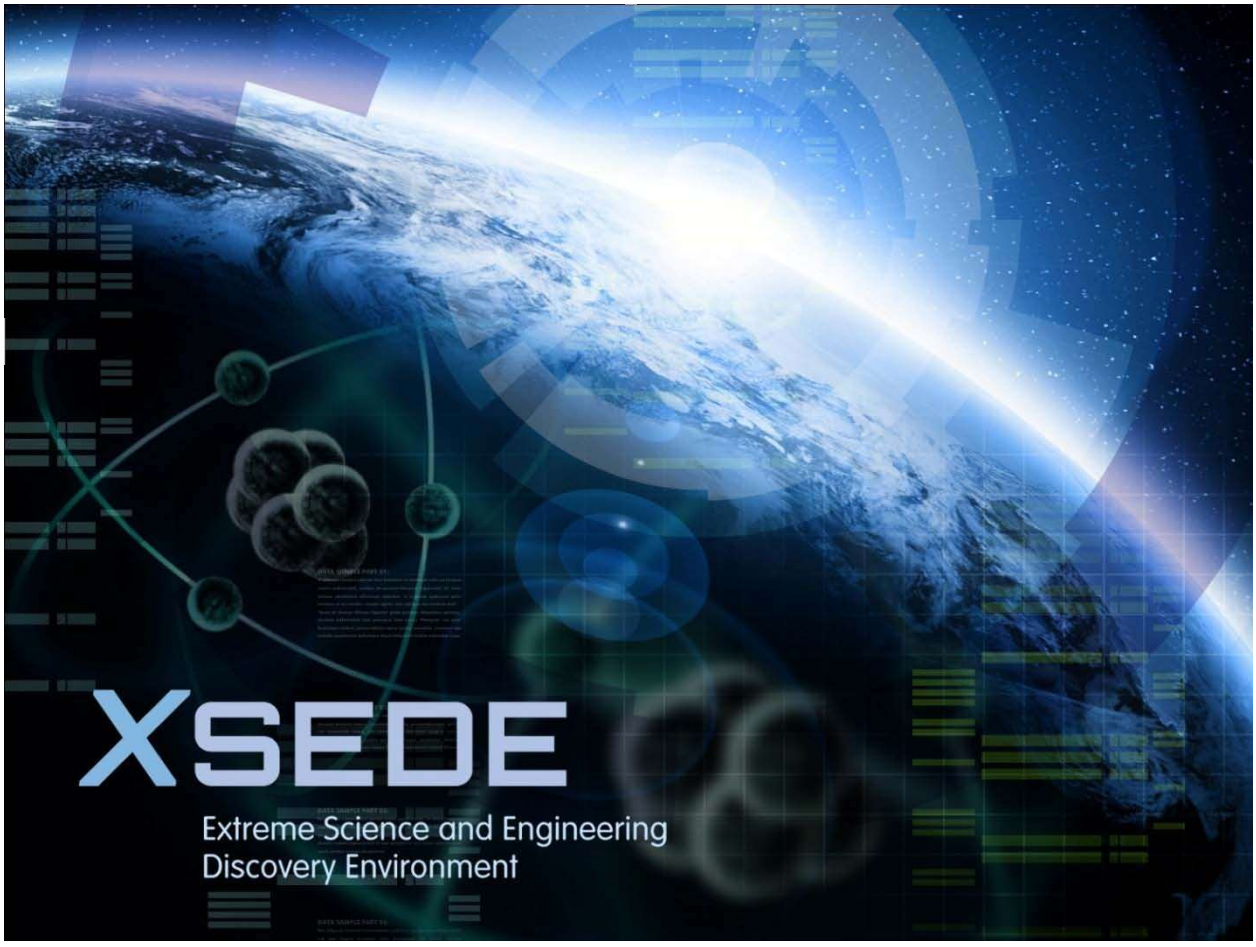
A XSEDE PEP Supplement: Cybersecurity Plan

Version 2.0

June 27, 2016



B Table of Contents

C XSEDE Cybersecurity Plan

XSEDE will be an open cyberinfrastructure that enables and supports leading-edge scientific discovery and promotes science and technology education. XSEDE will be comprised of NSF supported supercomputing and other systems located and managed by a variety of organizations around the country. These systems include large file and archival storage systems, visualization resources, data collections, workflow support systems, web services and science gateways connected by high-bandwidth nationwide networks. This highly integrated set of systems is coordinated through policies and operations, and supported by computational science and technology experts. Availability of the advanced digital resources and services is absolutely necessary to the productivity of the nation's research and education community. Such accessibility requires a balanced approach to cybersecurity that provides our nation's academic researchers continuous and reliable access to these resources.

XSEDE cybersecurity must support the confidentiality, availability and integrity of these resources by: following best practices, employing risk-based approaches, fostering teamwork throughout the XSEDE team, and integration of new proven cybersecurity technologies, procedures and approaches. The following sections document the XSEDE Cybersecurity Program Plan (CSPP), a comprehensive cybersecurity program for this distributed cyberinfrastructure. Rising to the top of this list are a number of strategies that include:

1. Support for a strong authentication and authorization service that limits access to only legitimate XSEDE users,
2. Coordination of the XSEDE cybersecurity staff among contributing XD and campus Service Providers to develop policies, design secure architectures and review risks,
3. Coordinated incident response and intelligence sharing across Service Providers, trusted partners and other federations,
4. A strong XSEDE cybersecurity education program, and
5. Proactive cybersecurity through careful risk/threat analysis, design and architecture of XSEDE at every level.

Cybersecurity in a highly distributed environment such as XSEDE is built upon the social networking and trust relationships honed over time among the partner cybersecurity staff. During PY6-10 XSEDE cybersecurity will build and improve upon a well-established community of security professionals and many of the successes of the XSEDE PY1-5 cybersecurity program. Successes during PY1-5 include the formation of an incident response team for the coordination of incident response across XSEDE sites and a broadened deployment of a cybersecurity architecture across the growing XSEDE user base. XSEDE will expand the cybersecurity team and draw on the expertise and experience of new individuals.

The XSEDE cybersecurity program will continue the effective cybersecurity program activities augmented with new thrusts broadening XSEDE's national impact including implementation of a two factor authentication for XSEDE users and providing secure gateway infrastructure and tools enabling more seamless transition from research groups and campuses to XSEDE resources. Improving security for existing services and building in security from the beginning for new services is an important part of this cybersecurity plan. Further XSEDE will undertake a risk/threat analysis that will guide how the security team applies its finite resources effectively. To oversee these efforts and provide a single point of contact and coordination of both internal and external security, the position of XSEDE Security Officer (XSO) will be continued. The XSO will serve as the responsible party for operational cybersecurity for XSEDE, advancements described in the defined cybersecurity mission and goals, and coordination with other XSEDE teams among other duties.

C.1 Cybersecurity Mission and Goals

The primary mission of cybersecurity in XSEDE is to provide for the confidentiality, availability and integrity of all XD resources, services and data, and to promote cybersecurity education for all XD users and staff. The mission will be accomplished by:

1. Performing risk/threat analysis,
2. Design, implementation and maintenance of cybersecurity in the XSEDE architecture,
3. Education, training, definition and implementation of best practices and,
4. The cooperation of XSEDE staff, Service Provider staff, other staff and end users to make cybersecurity a part of their everyday accomplishments supporting their job duties and scientific and research missions.

The activities towards achieving the goals of cybersecurity in XSEDE will be coordinated and directed by the XSO with support from the Security Operations and Coordination (SOC) team. The goals of cybersecurity in PY6-10 for XSEDE will build on the previous successes of XSEDE cybersecurity and will include new goals recognized as important to the cybersecurity of XD resources, services and data.

The goals of cybersecurity in XSEDE include, but are not limited to:

1. Following best practices
    a. Develop, maintain and secure approval of XSEDE policies, standards and guidelines
    b. Educate staff and end users on the secure access and use of XD resources, services and data through cybersecurity education, outreach and training
    c. Monitor the security posture of XD resources and services
2. Employing risk-based practices,
    a. Proactive cybersecurity through careful risk/threat/cost analysis, design and architecture of XSEDE at every level
3. Fostering teamwork among XSEDE security staff
    a. Coordination of the XSEDE cybersecurity staff among contributing XD and campus Service Providers through the SOC and other methods,
    b. Provide adequate and timely response to security incidents, including any improvements to incident response process, practices and tools
4. Integrating new proven cybersecurity technologies, procedures and approaches
    a. Improved cybersecurity posture including the elimination of plaintext passwords where possible and support and promotion of multi-factor password technology
    b. Provide secure frameworks for science gateways and workflows including community accounts
    c. Provide a flexible, yet integrated, cybersecurity authentication infrastructure including authentication with X.509 certificates and use of InCommon Federation services for integration into research groups and university campuses, and other capabilities

C.2 Roles and Responsibilities

This section defines the cybersecurity roles and responsibilities specifically for XSEDE cybersecurity leadership positions and generally for XD users and Service Provider staff.

XSEDE Security Officer (XSO)

The XSEDE Security Officer (XSO) will provide a single point of contact for both internal and external cybersecurity. The XSO will serve as the responsible party for XSEDE operational cybersecurity, maintenance of the XSEDE Cybersecurity Program Plan (CSPP), development (including obtaining management approval) and execution of policies, standards and guidelines, the advancements of the XSEDE cybersecurity mission and goals, review and evaluation of new cybersecurity technology for incorporation into XSEDE, coordination with other XSEDE teams, coordination with the XD Service Providers, risk/threat analysis, cybersecurity posture monitoring and improvements, incident response coordination with the SOC team lead, and incident response communication with XSEDE management and NSF. The XSO will work closely with the SOC lead to coordinate XSEDE cybersecurity issues to be discussed with the SOC team and will coordinate any internal and external security evaluations and reviews and report to XSEDE management on results of any such reviews. The XSO will participate and provide leadership on behalf of XSEDE to the InCommon Federation. The XSO will report to the XSEDE Operations Director for cybersecurity program progress and all other security matters. Matters of major incidents or significant cybersecurity policy changes will be brought to the attention of the XSEDE Project Director.

The XSO will be assisted by staff that will provide additional expertise including the identity management and grid authentication expertise of senior cybersecurity staff from the lead XSEDE partner organizations. These staff will work with the XSO to advise on XSEDE cybersecurity strategies and tactics. They will primarily be charged to assist the XSO in the design and implementation of a top-down cybersecurity approach as well as the assessment of emerging new security technologies.

Cybersecurity Operations and Coordination (SOC)

XSEDE will have a cybersecurity operations and coordination (SOC) team made up of representatives of the XSEDE partners, other XD service providers, other partners and key collaborators, as necessary. This group will meet regularly to discuss security items of importance for XSEDE.

XSEDE Staff and Service Providers

XSEDE staff and Service Provider staff have roles including: management and coordination of XSEDE, XSEDE project positions fulfilling a specific mission of the project, Service Provider management, Service Provider user support, Service Provider system administration and other roles. Members of these staff are responsible for providing for the confidentiality, availability, and integrity of data, resources and services of XD. Both XSEDE and Service Provider staff with privileges have an added burden of providing protection of their accounts and privileges due to the risk of unauthorized privilege escalation and the potential effect on XD. XSEDE staff and privileged users must follow XSEDE best practices and adhere to the policies, standards and guidelines of XSEDE.

Users

Users will make use of XD resources and services to accomplish their scientific and research mission and are expected to abide by the terms and conditions described in the XSEDE Acceptable Use Policy, any XSEDE user policies, and any Service Provider user policies. Failure to follow these can result in suspension of a user account or access to any specific resource where a violation has occurred.

C.3 Cybersecurity Operations and Coordination

Many members of the PY6-10 XSEDE security team have played important roles in the PY1-5 XSEDE security working group in developing and implementing security technologies and policies. Effective security among federated organizations requires the establishment of trust among the distributed team, which was a hallmark of the XSEDE Security Working Group. XSEDE will build on that foundation and continue the cybersecurity operations and coordination (SOC) team formed to coordinate operational cybersecurity activities, evaluate security technologies, and address incident prevention, detection and response across XSEDE. The partners on this proposal will form the core of the SOC along with other XD Service Providers, partners and key collaborators who are expected to participate (e.g. CERN, OSG, LIGO, and NERSC). The XSEDE Security Working Group will meet on a regular basis and discuss threats and vulnerabilities to XD resources, discuss, develop and perform new cybersecurity technology assessments and perform pro-active XD resource monitoring and reporting, address cybersecurity questions or issues from other XSEDE teams, and perform cybersecurity incident response as necessary. Working with the XSO, the XSEDE Security Working Group will periodically be charged by the XSO to review security policies, procedures, standards, guidelines and security-related implementation issues in order to make recommendations to the XSO regarding security policies and practices that should be adopted by XSEDE. The XSEDE Security Working Group will work with other XSEDE teams as necessary to review and address cybersecurity implications of software, services, and policies developed in those working groups. The SOC will review and make recommendations to the XSO in development of any cybersecurity trust relationships. The XSO will maintain a liaison with each of the other XSEDE teams.

The XSEDE Security Working group will build on XSEDE cybersecurity incident processes and procedures both to avoid incidents and define the incident response process including any coordination with local law enforcement or FBI, as necessary. Secure communication capabilities including web-based and email based will be employed for discussion and communication of sensitive security incident information. The XSEDE Security Working group will develop and maintain the XSEDE site cybersecurity contact directory and cybersecurity playbook. The team will proactively improve XSEDE cybersecurity through a risk assessment and mitigation process based on the latest standards and through adoption of cybersecurity controls where applicable.

The team will establish XSEDE-wide coordinated incident detection and proactive application of vulnerability scanning, e.g. using tools such as Qualys. Vulnerability scanning will be available centrally and will always be coordinated with the individual resources owners. The team will augment the procedures established in XSEDE with key advancements including a centralized mechanism for blocking a user account across XSEDE. Further, the XSEDE cybersecurity team will actively explore integrated and distributed intrusion detection system (IDS) technologies with an eye towards deployment throughout XSEDE.

C.3.1 Incident Response

As with any security program it is critical to have a skilled Incident Response team to rapidly respond and recover from cyber attacks. The Incident Response (IR) team (part of the SOC) will be available 24×7 to address any information security threat against XSEDE. The IR team will share the same expertise that developed the XSEDE Incident Response team. The IR team will have an array of secure and redundant communication and information sharing tools at their disposal. This will include a secure wiki that has an integrated secure ticketing and secure messaging system so that all incidents and communications in this highly distributed environment can be tracked and monitored by all authorized parties in a secure fashion. A 24×7 ‘Hotline’ will be maintained to support IR team coordination via standard telephone connections, in addition to a notification service to push out critical warnings and event notices, as well as support for encrypted e-mail.

Members of the XSEDE IR Team will share membership in information security sharing communities such as REN-ISAC, Grid-SEC, FBI Infraguard, and the TAGPMA IR-RAT. Participation in these communities will provide the IR team knowledge of the latest exploits and attack trends seen in the wild. The XSEDE IR team brings many years of experience in responding and recovering from real-world threats against many of the nations' high visibility resources.

C.4 Cybersecurity Awareness, Training and Outreach

Cybersecurity training will be improved and provided to those that use, develop, manage and administer XSEDE resources, services and data. For users a wide range of security awareness is needed. Making end users aware of items such as the XSEDE security tools and capabilities available, data integrity protections available, protecting authentication credentials and authentication and access control for campus bridging will be addressed via online and other electronic instructional materials and through in-person training and awareness sessions at XSEDE workshops, training and other events. Security awareness programs will be developed and presented to XSEDE users, science gateway and workflow developers and XSEDE and service provider staff for the protection of the resources and including additional awareness and protection measures for those who have privileges across XSEDE.

To broaden impact on the national community, XSEDE cybersecurity training will be integrated with and provided alongside all other XSEDE training resources via the XSEDE User Portal. In addition, the XSEDE project will engage the security research community by collecting and publishing XSEDE's security requirements to facilitate a research focus on security challenges relevant to NSF science researchers, computational grids and data grids.

Specific training classes to be developed include an *Introduction to Cybersecurity in the XSEDE Cyberinfrastructure*, *Cybersecurity for XSEDE Staff and Privileged Users*, and *Securing XSEDE Science and Engineering Gateways*. Additional security training courses will be provided as needed and at the direction of the XSO.

C.5 Policies, Standards, Guidelines and Procedures

XD sites and resources will be integrated in a manner that involves trust relationships, common potential threats and vulnerabilities, and a common set of users. As an integrated, national resource, XSEDE will have common authentication and access control methods, common name spaces, globally accessible resources along with a public perception of being a single unified entity. These commonalities give rise to the requirement that XSEDE policies, standards and guidelines (PSG) must be developed and maintained to influence user and staff behavior, dictate authentication and access control methods and implementations, provide for privileged and unprivileged user best practices and define the processes and procedures for incident handling. XSEDE PSGs will be reviewed and carried forward from XSEDE. Any missing PSG documents will be developed by the XSO or the SOC as directed by the XSO. The following PSGs exist at the end of XSEDE:

- XSEDE Acceptable Use Policy
- Security Working Group Charter
- Central Services Baseline Security Standard
- Science Gateway Security Policy and Guideline

- Privacy Policy
- Level 1 Service Provider Security Agreement
- XSEDE Certificate Service

C.6 Cybersecurity Posture Monitoring and Assessments

The XSEDE security team will undertake a risk/threat analysis of XSEDE leading to the development of a top-down approach to cybersecurity that follows the latest standards, guidelines and procedures, and further assess new technologies with an eye towards adoption.

C.6.1 Vulnerability Assessments

XSEDE will make available the Qualys vulnerability assessment tool to the members of the project for their use in periodic vulnerability assessment. The members will be allowed to use the tool to assess their resources and will be encouraged to do so on a regular basis.

C.6.2 Federated Intelligence Sharing

The XSO will oversee the deployment of a new system to share indicators of compromise and other intelligence automatically. This will start with the XSEDE2 Service Providers and expand to other partners in the XSEDE SOC, such as CERN and LIGO. This activity will also integrate with the Science DMZ security appliance being developed by XSEDE lead partners for small and medium-sized campuses around the country, serving as a place to analyze the many new intelligence feeds centrally.

C.6.3 Risk Assessments

On or by program year three, the XSEDE security team will conduct a comprehensive or targeted risk assessment, based on the ISO 27001 family of guidelines or the National Institute of Standards and Technology special publication (NIST SP) 800-53 as part of an overall, comprehensive, continuous improvement of XSEDE cybersecurity. The risk assessment will evaluate the current cybersecurity posture, what cybersecurity controls are in place, the effectiveness of the security controls and the gaps in cybersecurity as opportunities for improvement. The risk assessment will provide the foundation for improvement to the overall XSEDE Cybersecurity Program and for the identification of new technologies than may need to be evaluated. Results from the risk assessments will be analyzed and mitigation plans, if any, will be developed to minimize any identified high priority risks.

C.6.4 Cybersecurity Audits

The XSO in cooperation with the SOC team will request internal cybersecurity audits on, at least, an annual basis in order to assess specific technical aspects of the posture of the XSEDE project as a whole. These audits may include items of significant interest as discovered by a (recent) security incident or as a general cybersecurity spot check of known high-risk threats and/or vulnerabilities either generally known or recently discovered. An example includes contacting all resource providers to request their current status of the installment of a patch for a known, exploitable local or remote root compromise for a particular Linux kernel. Preparedness exercises will be conducted to identify and work out process issues and to test the overall security preparedness of the team to respond to actual incidents.

Additionally, XSEDE will conduct one or more periodic security reviews at the direction of the XSO and performed by an external review team. This external security review will evaluate the XSEDE security posture and make recommendations to improve XSEDE cybersecurity readiness. The external review team will be issued a charge by the XSO and shall provide a written report of the evaluation, findings and

recommendations. Areas that could be covered are listed, but not limited to, the security component areas from the NIST 800-53 document and the assessment criteria listed in NIST 800-53A.

C.7 New Technologies

New cybersecurity methods and technologies will be evaluated on an ongoing basis. Entry points for the identification of new technologies include, but are not limited to, the XSO and assistants, SOC team members, service provider system administrators, and XSEDE member security officers. New cybersecurity technologies will be evaluated by the XSO and assistants and employing the XSEDE engineering processes to determine usability in XSEDE.

Recommendations for inclusion of new cybersecurity technologies into XSEDE will be brought forward to the XSEDE management by the XSO and the TIS team. Retirement of outdated, vulnerable, or otherwise ineffective security technology from the architecture will also be reported to XSEDE management.

The elimination of plaintext passwords from XSEDE, where feasible, and the substitution and use of the XSEDE two factor authentication and evaluation of two factor authenticated certificates will be promoted for use by XSEDE enterprise services and end-user use at SPs. It is not intended for two-factor authentication to be the only authentication method available with XSEDE, but to be an option available for widespread use and also intended to be used as an authentication mechanism for incident response to known user and system compromises.

C.8 Secure Frameworks for Science Gateways and Workflows

XSEDE plans to continue the work of XSEDE to increase the visibility and support of the capabilities and numbers of science gateways and associated workflow support systems. As development and use of science gateways and workflow support systems increase throughout the life of XSEDE, the security implications of gateways must be addressed. These will be addressed through security evaluation and analysis, development of cybersecurity best practices guides, and communication directly with the gateway and workflow developers. Security must be addressed in the early design and in the continuous development of gateways and workflow systems.

The XSEDE cybersecurity program will build upon the successes and security knowledge of the XSEDE project to identify security threats and vulnerabilities of portal, gateway and workflow toolkits, provide solutions and mitigation plans to reduce the risks and develop a comprehensive plan for education and cybersecurity support for gateway and workflow users and developers. The plans will include education of users on the supported workflow engines, web service toolkits, legacy toolkits, authentication methods, communication of the overall systems architecture plan for gateways and workflows, and the secure frameworks available to gateway and workflow developers.

C.9 Metrics

XSEDE will collect and report on cybersecurity metrics with an emphasis on incidents, security measures deployed, authentication and access, and security awareness. See the XSEDE Operations section for the list of the XSEDE cybersecurity metrics.

C.10 Summary

This Cybersecurity Program Plan provides an overview of the requirements of the cybersecurity mission and goals, roles and responsibilities, management commitment, coordination among the XSEDE entities and the major program components. The CSPP is a living document that will be updated at least annually and more frequently as necessary. The XSO will update and maintain the CSPP. The CSPP describes the program management categories that will be adopted by XSEDE from the applicable recommendations of the National Institute of Standards and Technology special publication 800-53 as appropriate for an academic research cyberinfrastructure. XSEDE will be the most powerful open science infrastructure in the world; the XSEDE CSPP will ensure that it is the most secure and effective tool for computational research.


XSEDE