Response to Request for Comments National Science Foundation

Eric Cross – Information Technology Manager, National Solar Observatory
3665 Discover Drive
Boulder, CO 80303
ecross@nso.edu
(303) 735-7125

The NSF Major Facilities Guide (MFG), Section 6.3

I appreciate the opportunity to provide comments to the National Science Foundation in response to its request for comments on the next release of the NSF Major Facilities Guide. I hope to provide clear feedback for your review. Please feel free to reach out to me should you have any questions.

Section 6.3 - GUIDELINES FOR CYBER-SECURITY OF NSF'S MAJOR FACILITIES

6.3.1 Introduction

"Data creation, sharing, and analysis are central to the progress of science. As information has becoming increasing digital and increasingly accessible from anywhere, the confidentiality, availability, and integrity of information and information systems has raised the importance of cybersecurity considerations. Cybersecurity protects the availability of instruments and systems; promotes trust in, and availability of, data; and provides confidence in the integrity of the research resulting from use of facility information and information resources. At the same time, inappropriate, inefficient, and ineffective cybersecurity compliance regimes can be costly in time, human capital, and funding. Cybersecurity programs for a facility must appropriately balance risk with cost and research innovation. Thus, a cybersecurity program is based on a structured approach to planning, developing, and maintaining levels of information security and risk appropriate to a facility's mission and phase. A cybersecurity program should be scoped to the key assets, resources, and the full lifespan of the facility. It is necessarily a living program that adapts, adjusts, and advances. As such, cybersecurity programs require reporting, evaluation, and updating of the program as appropriate."

Eric Cross Comment: Agreeable introduction and setup for the content of the entirety of Section 6.3.

6.3.2 Major Facility Cybersecurity Program

"Uniform Guidance §200.303 states that the Recipient's internal controls, including technology infrastructure and security management, should be compliant with guidance published by the Comptroller General or Committee of Sponsoring Organizations of the Treadway Commission (COSO). Further, the Cooperative Agreement Supplemental Financial & Administrative Terms and Conditions (CA-FATC) for Recipients of Major Facilities or Federally Funded Research and Development Centers (FFRDC) requires an information security program and identifies a modest set of required components for the program. Additionally, an information security plan is a required element of the Project Execution Plan (PEP) per Section 3.4 of this Guide. The foundation for developing and maintaining a project's cybersecurity program lies in the research mission and goals of the facility itself. Related foundational considerations are project phase, size, complexity, project budget, and the project's required data management plan which identifies key information assets. In addition, geographic and institutional distribution can be an important overall factor. The three pillars of a cybersecurity program which rest on this foundation are governance; resources; and controls. Like other facility project components, the cybersecurity program should be appropriately represented in standard project documents and NSF oversight activities such as the project execution plan, project risk management plan, project budget, project reports, and project reviews. The

following sections define and describe a suggested framework for the facility cybersecurity plan. This framework is based on the previously mentioned three pillars of information security programs: Governance, Resources, and Controls. Major Facilities may use these pillars as a framework for founding, operating, evaluating, and improving their information security programs, and meeting the award terms and conditions. Since there are interdependencies among the pillars, an integrative approach is required. The exact content and emphasis of the information security program should be tailored to the mission, phase, size and scope of an individual facility. The three pillars of a cybersecurity program rely on a project-specific inventory of "information assets" to be protected. Risk-based approaches to protection of information assets are further determined by a project-tailored "information classification" which recognizes varying degrees of value, priority, and/or sensitivity of the information assets. The information asset inventory and information classification are described in the Controls section."

Eric Cross Comment: My interpretation of the MFG is that it is inherently directed towards NSF supported Large Facilities (LFs). I believe LFs are all sizeable programs with complex Information Technology Infrastructures. As such, I feel the NSF's commentary here provides too much leeway to the LFs to define the size and scope of their information security program. In this case, I expect wide-ranging implementations of security practices across all NSF LFs. As a result, an example of cybersecurity difficulty would be requesting all LFs to deploy a critical security requirement. Should a security change be mandated, impacts of deploying the changes will vary greatly across the LFs, and could potentially cease work.

As a real-world comparison, within Department of Defense (DoD) Programs, regardless of size (whether a single laptop, or thousands of computer systems), all programs must follow similar security program pillars – governance, resources and controls. These pillars are well-defined and provide program contractors specific information to implement these pillars, following detailed rules (not guidance), leaving little interpretation to the contractor. Within DoD Programs, information security programs will have little variance, and blanket modifications can be implemented with consistent impact across programs.

6.3.3 Governance
"Recommended governance elements for cybersecurity programs include: roles and responsibilities; policies and practices, risk acceptance and management."

6.3.3.1 Roles and Responsibilities
"Successful cybersecurity programs require an active role for facility leadership in policy development and implementation, assigning information asset ownership, and accepting residual risk.

A second essential role is that of information asset owner. This is a person, position, or entity given formal responsibility for an information asset (or set of assets) within an organization. There are typically multiple information asset owners. The asset owner understands the risks to the asset and ensure adequate controls are in place over the life of the project.

In addition, most cybersecurity programs identify a senior security role, such as a Chief Information Security Officers (CISO) or Information Security Officer (ISO) as owner of the cybersecurity program and lead decisionmaker for operational aspects of the cybersecurity program. This individual also facilitates the formation of informed cybersecurity policies, practices and risk management decisions by facility leadership and information asset owners."

Eric Cross Comment: While these recommendations and definitions are accurate and positive, I feel this is guidance (not mandates) that leaves these recommendations as options, open to acceptance or rejection by the LFs. I would prefer to see that each LF is mandated by the NSF to fill these roles and responsibilities, due to their importance to an overall security program.

6.3.3.2 Policies

"Every facility project with information assets will require the development, approval and implementation of some information security policies within its cybersecurity program. Policies are driven not only by the facility's information assets and classifications, but also by relevant regulations. Regulations may be international, national or local. Regulations may be specific to an information asset (e.g. HIPAA, FERPA, etc.) or to specific needs of a facility collaborator or user (e.g. ITAR, FISMA). Examples of common policies include: Acceptable Use Policy; Access Control Policy; Incident Response Policy. Sample templates may be found at the Trusted CI website. Trusted CI's guidance recommends developing a "Master Information Security Policy & Procedures" (MISPP) document as an initial policy-making step. A master policy provides an overview of the project's information security program including a summary of roles and responsibilities, as well as an organized list of specific information security policy documents. Additional sources of policy templates and forms include the Higher Education Information Security Council (HEISC) Resources Center, and SANS Institute's Information Security Templates page. Using example and template policies can streamline the policy production process, even if substantial customization is warranted. The policies themselves only reduce risk if attached to other elements of the cybersecurity program (e.g. roles and responsibilities, controls) and integrated into overall project governance and management."

Eric Cross Comment: A stronger message would be for the NSF to adopt TrustedCI policy templates, and provide them directly from NSF accessible resources.

6.3.3.3 Risk Management and Acceptance

"Cybersecurity programs employ a risk-based approach to information security and as such, there is inherent acknowledgement by NSF that any valuable activity requires acceptance of residual risk. Residual risk is that risk that remains in the presence of controls. An important output of a risk-based information security program is a documented set of well-informed risk management and project leadership acceptance decisions. Due to the rapidly changing technology landscape, a flexible, informal risk assessment process is often more valuable than a formal, detailed risk assessment that is out of date long before it is completed. In addition to the Center for Trustworthy Scientific Cyberinfrastructure (CTSC) guide which is tailored to the scientific community, the Open Science Risk Profile Working Group (OSCRP), has developed and released a "best practices" document to assist NSF, NIH and DOE projects in assessing cybersecurity risks related to Open Science projects. Finally, the Armed Forces Communications and Electronics Association International (AFCEA)'s I Cyber Committee has produced a useful and relevant publication: The Economics of Cybersecurity, A Practical Framework for Cybersecurity Investment."

Eric Cross Comment: I am not confident LF leadership will acknowledge the importance of Risk Management and Acceptance of their security programs based on the commentary in section 6.3.3.3. I feel this important task could easily be ignored, or set aside, due to the lack of any NSF published requirement. LFs leadership is focused on their scientific project, and if they are not required to accomplish an information technology security related task, I would expect little effort and few resources being available to LF Cybersecurity/Information Technology teams for these types of activities.

6.3.3.4 Evaluation

"Given the dynamic technology and cybersecurity landscape, organizations are advised to plan for periodic evaluations of the cybersecurity program, including policies, practices, and controls. While project management and NSF oversight will involve regular reporting and review of program milestones, outcome metrics, and incidents, the project is encouraged to consider periodic self-assessments, external or stakeholder reviews, and evaluation of incident response. Tools are available from variety of sources to aid in assessment."

Eric Cross Comment: I like the tone of this section. It does tend to conflict with the remainder of the overall section 6.3. All of section 6.3 is providing guidance of some sort, but does not

prepare or setup the LF for NSF oversight: security evidence/reports, review of milestones, metrics, incidents, etc. These are tangible NSF actions that I feel an LF cannot appropriately prepare for without specific actions, controls, etc. for the LF to fulfill. Simple example: If the NSF does not require minimum password complexity, how can an LF define password complexity to be compliant with NSF expectations during an NSF oversite exercise?

6.3.4 Resources

6.3.4.1 Budget
"Overall, worldwide cybersecurity spending is on the rise driven in part by response to increased cyber crime and new data protection regulations. There is wide variability in the cost of cybersecurity as a percent of overall IT budgets (3-12%) depending on the mission of the institution (e.g. Defense and Aerospace industries have more stringent requirements and proportionally higher costs.)) and size of the institution (Small institutions may not achieve economies of scale.). A secondary contribution to variability is the considerable discrepancy in what is within the cybersecurity budget as well as what is in the IT budget. A 2016 NSF Cybersecurity Summit examination of public data on DOE open science laboratory cybersecurity spending indicated that approximately 0.5% of the overall lab budget and 8-12% of the IT budget (excluding scientific IT) were spend on cybersecurity."

6.3.4.2 Personnel
"In addition to the CISO/ISO, ongoing access to skilled cybersecurity professionals is key to a successful cybersecurity program. The CISO may manage a team of dedicated information security professionals or oversee staff/activities in various departments within the facility.

Considering the demand for experienced cybersecurity professionals, organizations may need to consider outsourcing security services. In any scenario, information security resources outside the facility such as a parent institution/campus, peer organizations, commercial security consultants, intrusion detection and log monitoring services, and incident response services can be an important source of security expertise, training, evaluation, and recommendations.

In addition to technical skills, teaching skills, communication skills and negotiating skills are endemic to cybersecurity programs and are, therefore, necessary personnel considerations."

Eric Cross Comment: I do not understand the value of this section, and I believe it will be less useful to LF leadership. This may be a stretch, but I feel including comments about how the LF is required to include Cybersecurity funding line-items/work breakdown structure codes will have more impact. My feeling as an IT professional is that these funds should be included as separate/called-out "bucket" within all LF Cooperative Agreements between the NSF and the LF. Cybersecurity seems as-needed as every other aspect of the LF's construction and operations, so I would ask why are Cybersecurity funds not outlined and agreed upon during initial LF support by the NSF? The current Cooperative Agreement Supplemental Financial & Administrative Terms and Conditions (CA-FATC) for Recipients of Major Facilities or Federally Funded Research and Development Centers (FFRDC) are far too vague for LFs to implement security programs that the NSF (or outside security consultant) could review comparatively.

6.3.5 Controls
"Information security objectives, and controls, center on confidentiality, integrity and availability. Controls are designed to the facility's portfolio of information assets and aligned to the corresponding information classification for those information assets."

6.3.5.1 Information Asset Inventory
"Organizational identification and location of information assets is a prerequisite to competently securing those assets. See, CIS Critical Security Controls 1 and 2, and NIST 800-53 control CM8. The inventory might include many details, but at a minimum it should identify the asset and indicate the value or sensitivity of the system and/or classification of the information. The facility data management plan which is a required document for proposal submission is a key source for both asset identification and classification.

The asset inventory can be built by manually using publicly or commercially available templates or worksheets or by constructing a custom database. The Open Science Cyber Risk Profile (OSCRP) provides guidance on assets to consider for science projects. Trusted CI has developed substantial guidance for information security programs in NSF projects, including a template for recording data about information assets. To reduce the manual effort, security products or scanners can aid with asset discovery and inventory.

Information is any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. Organizational information may be stored and used within the organization's information systems, as well as flow out to third party systems.

An information system is a discrete set of information and related resources (such as people, equipment, and information technology) organized for the collection, processing, maintenance, use, sharing, dissemination, and/or disposition of information. These include, but are not limited to, mobile devices, computers, networking systems, as well as industrial control systems (ICS) / supervisory control and data acquisition (SCADA) systems, physical security systems, heating, ventilation, and air conditioning (HVAC) systems, and any other connected devices or instruments."

6.3.5.2 Information Classification
"Information has varying degrees of organizational value, sensitivity, and protection requirements. These qualities are key factors to consider in analyzing the anticipated impact of security incidents. In addition, some information assets may be subject to additional external control (e.g. federal or state privacy laws, international regulations, contractual obligations). In most cases, information can be classified into two to four categories (e.g., public, internal, and controlled)."

6.3.5.3 Control Set
"Controls or mitigations are the administrative, technical, and physical safeguards and countermeasures implemented to support the facility's mission and ensure the appropriate protection of information assets. Control selection, implementation and evaluation are ongoing processes in any information security program. While efficiency and effectiveness will require customization of controls, there are several authoritative sources to assist in selecting baseline controls. Scientific facilities may merit special security considerations (e.g. diverse research data flows; identity management for distributed science communities ; non-facility device connectivity to facility networks and data; unique Industry Control (ICS) and/or Supervisory Control and Data Acquisition (SCADA) systems6; application software development)."

Eric Cross Comment: I like calling out these controls, assets and information classification guidelines. This section, 6.3.5, is the heart of what a LF Chief Information Security Officer would be looking for from the NSF to ensure their LF was maintaining a proper Cybersecurity program, with respect to the NSF. In my position, I would hope there would be a control set requirement guide, with specific and detailed controls, that mandated LF's compliance. I believe stronger wording, with accountability, would move LFs toward better overall security posture. Even if the NSF does not now have a mechanism to be the Cybersecurity "Police", having the requirements in place for LFs to implement would be extremely beneficial. This would arm LF Cybersecurity and Information Technology professionals with a minimum set of security controls to deploy across the LF's infrastructure. In this scenario, LFs could collaborate within a cybersecurity control set 'language' that is recognizable across the entire NSF landscape.

Currently, LFs can only discuss how to deploy certain technologies. As it stands now, LFs cannot help one another with deploying specific technologies and mechanisms to ensure their information security program controls are meeting NSF defined/blessed Cybersecurity settings and requirements.