U.S. National Science Foundation

RESEARCH INFRASTRUCTURE GUIDE (RIG)

Digital Backbone

Navigating RIG Revisions to Cyberinfrastructure & Cybersecurity

Bill Miller, NSF Senior Advisor for Cyberinfrastructure
Michael Corn, NSF Cybersecurity Advisor for RI
Alison Rockwell, NSF Research Infrastructure Advisor

Mid-scale RI Image Credit: Ohio State University, Cornell University, Georgia Tech Research Corporation, Florida State University, Woods Hole Oceanographic Institution, The University of Kentucky Research Foundation, Arizona State University, NSF I-Corps Northeast Hub, the University of Arkansas, Georgia Institute of Technology, the University of Michigan, University of California-San Diego, and the University of Tennessee, Knoxville

Digital Backbone

RIG Revisions to Cyberinfrastructure & Cybersecurity

Session Overview

- Why revise this RIG content?
- Cyberinfrastructure
- Cybersecurity / Information Assurance
- Interactive Q&A Session

Digital Backbone

RIG Revisions to Cyberinfrastructure & Cybersecurity

Why?

- Rapid evolution of cyberinfrastructure (CI) and Cybersecurity / Information Assurance (IA) technologies and user expectations.
- Guidance in the RIG will benefit from updating and clarifying.
- Community input has highlighted key challenges reflected in the revisions.
- Ensures CI and IA remain aligned with the RI vision and science mission.

Cyberinfrastructure: Motivations for updating the RIG

- Cyberinfrastructure (CI) = digital resources and services enabling the science mission.
  - Computational, data, control, software and middleware, networking resources and associated cybersecurity; related policies, standards, protocols; staffing; and systems enabling interconnectivity with external resources, ….

    (Not general IT, which is covered under Information Assurance.)
- Current RIG entry for CI covers "cybersecurity", "code development", and "data management plan". The reality is much more involved…
  - RI projects are increasingly dependent on both internal CI and externally leveraged CI to accomplish their missions and accommodate new – and integrated – modes of science.
  - Technologies, user expectations/usage modes, interconnectivities, data policies and practices rapidly evolve across the RI lifecycle.
  - This is an area where issues and challenges are commonly encountered during project implementation and operations.
- NSF wants to clarify expectations about CI across the CI life cycle.

Cyberinfrastructure: Approach

- NSF is considering requiring a Cyberinfrastructure (CI) Plan for new Major Facilities and Mid-Scale RI - updated throughout the project lifecycle.
  - Existing RIs would be encouraged to craft a CI plan going forward, as applicable.
- To keep this as simple but clear as possible, the approach would be:
  - Assume that the various project documents (PEP, WBS, budget, annual work plan, DMP, etc.) should contain the required CI-related information.
  - The CI Plan template will define the areas that (at a minimum) should be found/addressed in those documents (as appropriate). [next slide]
  - The completed CI Plan has brief narratives and pointers to that information in the other documents.
- The CI Plan can thus serve as a roadmap/checklist for the RI team, NSF PO, and reviewers, and be updated as the life cycle progresses.

Cyberinfrastructure: Areas to address, as applicable [draft]

Summary of how the CI will enable the science mission	• Concept of scientific use (target user base, utilization model(s), etc. • Summary of architecture, functionality and operational modes • Anticipated data products and data life cycle.
Summary of CI elements and associated technical, functional, and performance requirements	• **Internal CI** (built, controlled and/or owned by the project): Software, data, computational, networking and other internal systems, tools, and services. • **External CI**, facilities, and resources to be used or connected: Integration and interoperability requirements and dependencies on computational, data, networking, and other resources and services; associated access management systems. • **Cybersecurity systems and protocols** *related to the above CI*. (Would also point to the Information Assurance section as applicable).
CI implementation approach	• Summary of implementation management plan; in-house build vs. external leveraging • CI Quality Assurance; approach to user responsiveness; • CI staffing requirements and approach; summary of salient implementation risks.
CI operational approach	• CI performance monitoring and measurement, salient operations risks • CI refresh plan and approach • CI operations staffing and training plans.

Cyberinfrastructure Questions?

U.S. National Science Foundation

RESEARCH
INFRASTRUCTURE GUIDE (RIG)

Information Assurance Supplement to the Research Infrastructure Guide

Michael Corn
micorn@nsf.gov

Mid-scale RI Image Credit: Ohio State University, Cornell University, Georgia Tech Research Corporation, Florida State University, Woods Hole Oceanographic Institution, The University of Kentucky Research Foundation, Arizona State University, NSF I-Corps Northeast Hub, the University of Arkansas, Georgia Institute of Technology, the University of Michigan, University of California-San Diego, and the University of Tennessee, Knoxville

Note: pre-decisional preview

Individual comments only please – no guarantee of a response or adoption of suggestions (but I am incredibly grateful for everything and anything)

Send to micorn@nsf.gov

Problem Statement

The existing RIG language

- lacks specificity and actionable guidance
- is unclear about intended audience
- raises challenges (e.g., hiring) without suggesting any approaches to resolution
- lacks any rubrics for evaluating the success or completeness of a security program
- fails to address exigent changes in the threat or technology landscape
- fails to crisply articulate awardee obligations.

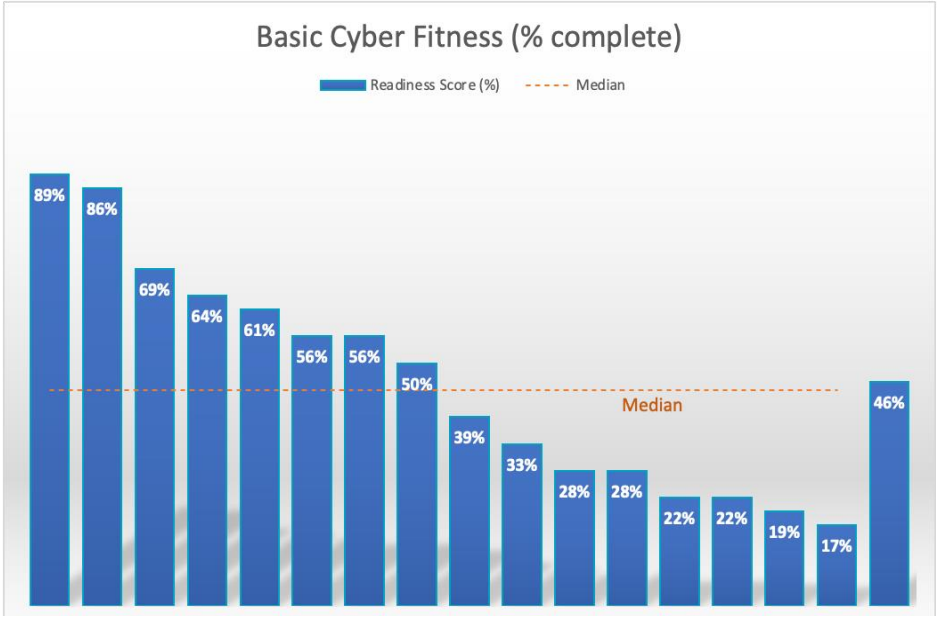
What's New?

- Refers to Information Assurance as the umbrella term for cybersecurity, privacy, data management, resilience
- Significantly expands guidance on building an information assurance program (a bit pedantic to be honest)
- Adds new reporting requirements for facility reviews (risk registers, budget, and "security plan" is now "information assurance management plan")
- Adds new expectations for security controls to be met*
- Makes additional recommendations to inform the information assurance program

* don't panic 😱

Why Not Panic about Control Requirements?

- Implementation time frame under discussion
- Evaluating possible costs for implementation
- Most major facilities are well on their way already



Goals & Structure

- Provide Program Officers and panels the information needed to assess cybersecurity
- Elevate cybersecurity to a first-class object of attention
  - Increase leadership engagement in cybersecurity at the facilities
  - Help leadership gain clarity on where to invest in cybersecurity
- Lean into foundational best practices without becoming too prescriptive

Outline of Supplement

- Intro
- Resilience
- Contemporary Threat Landscape

Framing

- Awardee Obligations
- Cyber Risk
- The Information Assurance Management Plan
- Critical Controls

Requirements

- Pillars of an Information Assurance Program
- Data Management and Curation
- IA and Cyberinfrastructure
- Cyberbreach Insurance
- Program Assessment

Recommendations / Guidance

Cyber Risk Register

Cyber Risks belong on the master project risk register

Cyber risks may be broken down into sub-categories, for example:

- Strategic Risks: for example, relevant geopolitical flareups; regulatory compliance; unmet budget or staffing needs.
- Exigent Risks: e.g., ransomware, supply chain, urgent and impactful vulnerabilities.
- Operational Risks: Unmet controls in any adopted standards, i.e., gaps in the baseline cybersecurity program.

Examples

- operational gaps in compliance with a chosen standard or set of controls, e.g., partially deployed MFA for remote access
- lack of resources allocated to address a risk
- failure to meet a regulatory obligation, e.g., NSPM-33
- exigent risks such as ransomware, spear phishing, or vulnerabilities in opensource software
- reputational risks to the facility, NSF, or the country due to outages or cyber incidents
- risk to national and international partnerships due to a loss of confidence in a facility
- risk to the continuity of operations
- risk to the integrity of scientific data or artifacts
- the discovery of illegal or unethical data in your AI/ML training data

Cyber Budget

Resources. Information assurance programs require adequate resources. The percent of project budget that most large facilities devote to information assurance covers a wide range and is tightly coupled to the type of facility. A mature facility will be able to line item the information assurance budget, avoiding the common practice of embedding Information Assurance expenses in technology or cyberinfrastructure budgets. The security budget as a percentage of total budget for a ship, for example, may be wildly different than a monolithic computational facility.

Examples

- Firewalls
- IDS / Honeypots
- Endpoint security software
- MFA solutions
- Staff (fractional and full time)
- Consulting

- Upgraded networking equipment to address cybersecurity
- IAM enhancements
- Logging (that supports security & operations)

Information Assurance Management Plan

Created by the major facility or mid-scale infrastructure's IA Lead, the IAMP is the high-level management 'runbook' for an information assurance program. It is not a collection of policies and procedures but a place to codify an information assurance program's scope, roles and responsibilities, governance, and controls. Regardless of how the RI chooses to entitle or structure its IAMP, do not lose sight of the fact that the IAMP is a tool for management. The IAMP can reference large bodies of policies, processes, or control sets but are distinct artifacts.

The information assurance lead, typically entitled an Information Security Officer, is the individual accountable for the entire execution of the IA program. RI management should expect their IA lead to participate in cross-RI communities and programs. NSF recommends including the IA Lead on the executive management team.

Sample IAMP Contents

- Statement of cyber risk management strategy (chosen framework and control set)
- Scope and Boundaries
- Responsibility Model and Matrix
- Governance
- Resource Plan
- Risk Treatment Plans
- Program Operations
  - Programmatic Processes
  - Baseline Security Functions
  - Supplemental Responsibilities
- Assessment Plan

Expectations for Feedback

Questions, suggestions, and feedback send to micorn@nsf.gov.
Individual comments only please – no guarantee of a response or adoption of suggestions (but I am incredibly grateful for everything and anything)

- What in this new/revised section is not clear?
- What key elements of NSF guidance are missing?
- What is too jargony, needs unpacking, needs gentler/stronger language?

Slide Bank

Cyber Fitness Control Set

Control	Priority Family
Require Multi-Factor Authentication for all privileged/administrator accounts	Urgent
Require Multi-Factor Authentication for all remote access	Urgent
Require Multi-Factor Authentication for all applications	Urgent
Defined process for identifying, tracking, and remediating vulnerabilities	Urgent
Hardening standards / processes for critical infrastructure	Urgent
Limited scope privileged/adminstrator accounts	Critical
Immutable backups of systems	Critical
Immutable backups of essential research data	Critical
Network segmentation and isolation	Paced
Regular tests of back up integrity testing of restoration process	Paced
Incident Response Plan and annual tabletop exercise simulating a major incident	Paced
Collect and monitor all system logs	Paced
Maintain and update an inventory of critical infrastructure	Paced
Deploy and maintain anti-malware software	Paced
Anti-malware includes Endpoint Detection and Response (EDR) functionality	Paced

NB: Priorities are merely a recommendation

2023 Infrastructure Workshop Comments / Observations

Generally, respondents were CI/CS practitioners

- Requested greater specificity
- Requested NSF to ”pick a standard”, e.g., CUI. (CUI was called out as the future standard)
- Frustration was expressed that CS costs are not fully baked into budgets
- Frustration expressed that CS demands increase but CS budgets do not
- Hope was expressed that greater specificity in CS requirements would result in more engagement of senior project leadership and CS

Digital Backbone

RIG Revisions to Cyberinfrastructure & Cybersecurity

Recap

- Cyberinfrastructure and information assurance is rapidly changing, and guidance needs to keep pace.
- The RIG guidance on CI and IA will be streamlined and updated to reflect current needs.
- NSF is considering including guidance on a CI Plan and an IA Management Plan.
- Note: New RIG planned for publication in early 2025.

Digital Backbone

RIG Revisions to Cyberinfrastructure & Cybersecurity

Feedback is welcome

- For **Cyberinfrastructure**, contact
  - Bill Miller, wlmiller@nsf.gov

- For **Information Assurance**, contact
  - Mike Corn, micorn@nsf.gov

Questions?


U.S. National Science Foundation
WHERE DISCOVERIES BEGIN
RIG
RESEARCH
INFRASTRUCTURE GUIDE
NSF guidance for full lifecycle oversight of Major Facilities and Mid-scale RI
NSF Research Infrastructure Office
Office of Budget, Finance and Award Management