Date: 05 April 2021
From: Mr. Craig Jackson, Mr. Bob Cowles
To: Ms. Suzanne Plimpton
Cc: Mr. Von Welch, PI and Director, Trusted CI, the NSF Cybersecurity Center of Excellence
Re: Comments on Major Facilities Guide: Draft for Public Comment (December 2020)

Ms. Plimpton,

Please accept the following comments made on behalf of Trusted CI, the NSF Cybersecurity Center of Excellence. Do not hesitate to reach out to us if you have questions.

Comment 1

4.6.6-8, Information Technology Competency & Description (PDF p.199)

Recommendation: We are pleased to see knowledge of the Trusted CI Framework and cybersecurity programmatics referenced as a personnel competency. Consider updating this to include reference to the Trusted CI Framework's fourth pillar (Mission Alignment) and the Framework Implementation Guide for Research Cyberinfrastructure Operators. See, https://www.trustedci.org/framework.

Rationale: Please refer to our Comment 2 rationale regarding Section 6.3 GUIDELINES FOR CYBER-SECURITY OF NSF'S MAJOR FACILITIES.

Comment 2

6.3 GUIDELINES FOR CYBER-SECURITY OF NSF'S MAJOR FACILITIES (PDF pp.274-281)

Recommendation: We recommend NSF update Trusted CI resource references to point Major Facilities to the Trusted CI Framework and the Framework Implementation Guide for Research Cyberinfrastructure Operators. While NSF might choose to reduce the language of section 6.3 substantially by referencing this new guide, NSF should at least make the following updates:

a. 6.3.2-1, second, third, and fourth paragraphs. Add reference to the Framework's fourth pillar, Mission Alignment. Update footnote 4 to reference https://www.trustedci.org/framework.
b. 6.3.3.2, footnote 1. Update the reference to https://www.trustedci.org/framework/templates.
c. 6.3.5.1, footnote 5. Update footnote 4 to reference https://www.trustedci.org/framework.

Rationale: From 2014 to 2018 we collaborated with the Large Facilities Office to provide eight drafts of recommended content for what became the first and currently active cybersecurity section of the Major Facilities Guide (fka Large Facilities Manual). Those drafts represented an early distillation of the Trusted CI Framework (trustedci.org/framework). The section NSF ultimately published included references to Trusted CI's resources, including its 2014 Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects (trustedci.org/guide). It also included explicit references to 3 of the Trusted CI Framework's 4 Pillars (Mission Alignment, Governance, Resources, and Controls).

In March 2021, Trusted CI published the Trusted CI Framework Implementation Guide for Research Cyberinfrastructure Operators. This new guide supersedes the 2014 guide. Read more about the background, community vetting process, and release here: https://blog.trustedci.org/2021/03/published-trusted-ci-framework.html.

We believe NSF returning the Mission Alignment Pillar to the MFG will help avoid confusion in the community. While the section already has some emphasis on mission, community members have inquired with us as to why NSF omitted explicit reference. For this community, there is no greater purpose for cybersecurity than to enable scientific discovery.

Maintaining strong and up-to-date guidance on the importance of cybersecurity programmatics resonates with the recent JCORE report on research security.[1] The Trusted CI Framework's emphasis on mission, governance, leadership involvement, and appropriate resourcing echoes the report's charges to "convey the importance of research security and integrity at the leadership level" (Recommendation 1) and "ensure an organizational approach to research security" (Recommendation 2). A robust cybersecurity program would be an essential component of any comprehensive research security program (Recommendation 4). Moreover, the Trusted CI Framework is specifically designed to enable effective, efficient use of security controls like those described in the JCORE report (see, Recommendation 21).

Comment 3

6.3.3.3, Risk Management and Acceptance
(PDF p.278)

Recommendation: Correct the OSCRP reference to "Open Science Cyber Risk Profile (OSCRP) community project."

Rationale: The draft for comment is missing "Cyber" in the proper name.

Comment 4

6.3.5.1, Information Asset Inventory
(PDF p.280)

Recommendation: Add clarification that "information systems" includes both traditional information technologies (*e.g.*, servers, mobile computing devices) as well as operational technology (OT), *e.g.*, industrial control systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems.

Rationale: While the MFG references controls for ICS and SCADA systems in Section 6.3.5.3, a clarification of the scope of "information systems"is warranted. Our work with Large/Major Facilities since 2013 suggests that some community stakeholders believe cybersecurity and related responsibilities are scoped only to traditional IT, and do not include OT.

[1] https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/NSTC-Research-Security-Best-Practices-Jan2021.pdf

If reflected in the scoping and resourcing of theircybersecurity programs, this misunderstanding and exclusion of OT cybersecurity considerations poses a serious risk to facility research missions. These missions frequently rely heavily on operational technology. The availability, functionality, and efficacy of scientific instruments (*e.g.*, telescopes) frequently depend on both operational technologies and traditional information technologies. These technologies are increasingly architected as interconnected systems of systems composed of bothtraditional IT and OT. Cyberthreats to these operational technologies are real[2] and attacks that impact them can be executed both directly and through connected traditional IT systems. The gravity and impact of cyberthreats to OT is recognized at the federal level and action to address these threats is called out explicitly as a priority.[3,4,5]

This addition also will help clarify that NSF's guidance is aligned with the federal definition of cybersecurity.[6]

Very respectfully,

Craig Jackson
Program Director, Indiana University Center for Applied Cybersecurity Research
Senior Personnel, Trusted CI, the NSF Cybersecurity Center of Excellence
scjackso@iu.edu

Bob Cowles
Senior Fellow, Center for Applied Cybersecurity Research
Consultant, Trusted CI, the NSF Cybersecurity Center of Excellence
Principal, Brightlite Information Security
bob.cowles@brightlite-infosec.com bob.cowles@gmail.com

[2] See, https://www.dragos.com/resource/dragos-releases-annual-industrial-control-systems-cybersecurity-2020-year-in-review-report/.

[3] See, *e.g.*, NATIONAL SECURITY AGENCY CYBERSECURITY REPORT: NSA/CSS Technical Cyber Threat Framework v2, p.2. Available at https://media.defense.gov/2019/Jul/16/2002158108/-1/-1/0/CTR_NSA-CSS-TECHNICAL-CYBER-THREAT-FRAMEWORK_V2.PDF

[4] See also, NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems - Alert (AA20-205A), Original release date: July 23, 2020. Available at https://us-cert.cisa.gov/ncas/alerts/aa20-205a.

[5] See also, NSA press release, "Protect Operational Technologies and Control Systems against Cyber Attacks." Available at https://www.nsa.gov/news-features/press-room/Article/2285423/protect-operational-technologies-and-control-systems-against-cyber-attacks/

[6] https://fas.org/irp/offdocs/nspd/nspd-54.pdf