## Yasky, Rebecca Kay

**From:** Plimpton, Suzanne H.
**Sent:** Tuesday, February 19, 2019 10:41 PM
**To:** Yasky, Rebecca Kay
**Subject:** FW: [EXTERNAL] - Comments on Major Facilities Guide

Hi, Rebecca,

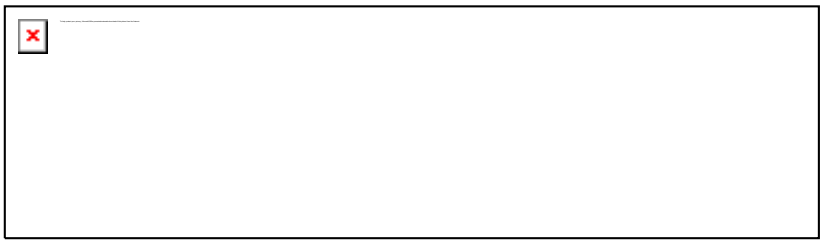
Here's another one. I'll be checking the Federal Docket Management System later to see if any comments came in via the Federal Register's online site.

Thanks,

Suzanne

---

**From:** Bob Cowles <bob.cowles@gmail.com>
**Sent:** Tuesday, February 19, 2019 7:05:08 PM
**To:** Plimpton, Suzanne H.
**Cc:** Craig Jackson; Von Welch
**Subject:** [EXTERNAL] - Comments on Major Facilities Guide



Trusted CI, the NSF Cybersecurity Center of Excellence, submits these comments in response to:

NATIONAL SCIENCE FOUNDATION Agency Information Collection Activities: Proposed Collection; Comment Request
AGENCY: National Science Foundation.
ACTION: Notice and request for comments.
Federal Register / Vol. 83, No. 245 / Friday, December 21, 2018 / Notices

The following comments apply to the previously reserved section on cybersecurity, now section 6.3 of the Major Facilities Guide (MFG). Questions or requests for clarification should be sent to Craig Jackson, *scjackso@iu.edu*

We are pleased to see NSF publish cybersecurity guidance for Major Facilities. In our experience working closely with Large Facilities via the Large Facility Security Team (LFST), one-on-one engagements, and at community events like the NSF Cybersecurity Summit, we know many cybersecurity and information technology practitioners at facilities have eagerly anticipated more guidance on cybersecurity expectations. Since 2014, we have collaborated with the Large Facilities Office to provide eight drafts of suggested content for this cybersecurity section of the Large Facility Manual (now Major Facilities Guide). We vetted the most recent Trusted CI drafts with the LFST. While the published draft provides less detail and specificity than our most recent drafts, we believe much of the content is well-aligned with Trusted CI's advice and experience working with the community. This MFG section will be well-aligned with the *Trusted CI Framework* and the companion *Trusted CI Framework Implementation Guide for Providers of Scientific CyberInfrastructure* we're developing as a follow-on to our Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects. That framework and its related products will

provide explicit requirements for what it takes to stand up and maintain a competent cybersecurity program that supports open science missions.

The following are our detailed comments and suggested changes or additions. The purpose of these suggestions is to aid in usability and readability, as well as alignment with Trusted CI's guidance to the community.

Detailed comments:

**1**
**Throughout the document**

**Suggested change:** Replace "information security" with "cybersecurity" throughout or define them as being equivalent terms

**Discussion:** Cybersecurity and information security - both used but not explicitly described as equivalent.

**Justification:** Clarity and consistency

## 2
## Throughout the document

**Suggested change:** Add page numbers to the document

**Discussion:** The lack of page numbers makes referencing or communicating about the text in the document more difficult.

**Justification:** Improve ease of communication about parts of the text.

**3**
## 6.3.1 Paragraph 1

**Suggested change:** Last sentence - strike "of the program"

**Justification:** redundant and awkward phrasing

**4**
**6.3.2 Paragraph 1**

**Suggested paragraph replacement text:**
A cybersecurity plan is a required element of the Project Execution Plan (PEP) per Section 3.4 of this Guide. Additionally, based on Uniform Guidance §200.303, to the extent the award recipient's IT infrastructure is integral to internal controls, the relevant portion of the cybersecurity program 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. [add footnote references where appropriate]

**Discussion:** The first paragraph is confusing since it is an amalgam of requirements from different sources with different scopes. We suggest moving the sentence with the broadest scope (the requirement for the PEP to include a cybersecurity plan) to the start of the paragraph. Next would be the requirement on the internal controls but reworded to narrow applicability to cases when internal controls implemented through information technology. Finally, close with the Cooperative Agreement Supplement(s). Note: Uniform Guidance §200.303 does not actually include the phrase "including technology infrastructure and security management".

**Justification:** The document now applies to more than Large Facilities or FFRDCs, so it adds clarity to state the requirements in order of scope. Also, clarifying the application of 200.303 to IT implementations of internal controls.

**5**
**6.3.2 Paragraph 2**

**Suggest changing the sentence** "The three pillars of a cybersecurity program which rest on this foundation are governance; resources; and controls."

**To read** " The four pillars of a cybersecurity program which rest on this foundation are mission alignment, governance; resources; and controls.

**Discussion:** While the "research mission and goals of the facility" are foundational, the actual alignment of the cybersecurity program is an additional pillar because the program elements there need to evolve in concert with the other pillars.

**Justification**: Adding the Mission alignment pillar will be consistent with the upcoming Trusted CI Framework.

**6**
**6.3.2 Paragraph 3**

**Suggest changing the sentence**: "This framework is based on the previously mentioned three pillars of information security programs: Governance, Resources, and Controls."

**To read:** "This framework is based on the previously mentioned four pillars of cybersecurity programs: Mission Alignment, Governance, Resources, and Controls."

**Discussion:** Alignment with changes suggested for paragraph 2

**Justification:** Consistent changes

**7**
**6.3.2 Paragraph 4**

**Suggest** inserting a new page formatting command

**Suggest changing the sentence**: "The three pillars of a cybersecurity program rely on a project-specific inventory of "information assets" to be protected."

**To read:**
**"6.3.3 Mission Alignment**

The other three pillars of a cybersecurity program rely on a project-specific inventory of "information assets" to be protected."
**Note:** Requires changing the numbering of subsequent sections and updating page headers/footers

**Discussion:** Add the Mission Alignment pillar

**Justification:** See above

**8**
**6.3.3.1 Paragraph 3**

**Suggest changing:** "In addition, most cybersecurity programs identify a senior security role …:

**To read:** "In addition, cybersecurity programs should have an identified senior security role …"

**Discussion:** Having an individual responsible for the cybersecurity program is important and should not be an undue burden. The task is not necessarily full-time but the core responsibility for the program should be centralized.

**Justification:** Strengthen the guidance to have individual primary program responsibility

**9**
**6.3.3.3 Paragraph 1**

**Suggest changing:** "Center for Trustworthy Scientific Cyberinfrastructure (CTSC)"

**To read:** "Trusted CI"

**Discussion:** CTSC has changed its name to Trusted CI.

**Justification:** Update organization name

**10**
**6.3.3.4 Paragraph 1**

**Suggest changing:** "... organizations are advised to plan for …"

**To read:** " … organizations should plan for …"

**Suggest changing:** " … the project is encouraged to consider …"

**To read:** "... the project should include in the NSF review …"

**Discussion:** Given that NSF oversight will require a review of the cybersecurity program, the language in this paragraph should be strengthened.

**Justification:** Ensure the cybersecurity program undergoes periodic evaluation and review

**11**
**6.3.4.2 Paragraph 3**

**Suggest changing:** "In addition to technical skills…"

**To read:** "While technical skills are important …"

**Discussion:** The sentence is easily misread due to the comma-separated list.

**Justification:** Better separation of "technical skills" from the other listed items

**12**
**6.3.5 Paragraph 1**

**Suggested paragraph replacement text:** "Controls are tailored to the facility's portfolio of information assets and aligned to protect confidentiality, integrity, and availability based on the corresponding information classification for those information assets."

**Discussion:** The paragraph is poorly worded or contains redundant information.

**Justification:** Better wording for the point being made.

**13**
**6.3.5.1 and 6.3.5.2**

**Suggested change**: Move the two sections under the Mission Alignment pillar and renumber the Control Set section. Make appropriate page header/footer alterations.

**Discussion:** The subsections now belong under Mission Alignment and should be moved entirely under that pillar.

**Justification:** These topics are part of the Mission Alignment pillar.