The government seeks individual input; attendees/participants may provide individual advice only.

Middleware and Grid Interagency Coordination (MAGIC) Meeting Minutes
November 15, 2022

Hybrid Meeting: SC22 – Dallas, TX

Participants

Dan Gunter (LBL)	Marcy Collinson (Oracle)
Davina Pruitt-Mentle (NIST)	Miron Livny (Wisconsin)
Eric Blanco (NCO)	Padma Krishnaswamy
Fouad Ramia (NCO)	Rob Beverly (NSF)
Hal Finkel (DOE/SC)	Rich Carlson (DOE/SC)
Jay Park (NSF/OAC)	Steve Wallace (Internet2)
Jim Basney (Illinois)	Thomas Maier (ORNL)
Mallory Hinks (NCO)	

Introductions: This meeting was chaired by Rich Carlson (DOE/SC) and Jay Park (NSF)

Trusted CI Update

Jim Basney

- Jim shared the mission of Trusted CI: to lead in the development of an NSF Cybersecurity Ecosystem with the workforce, knowledge, processes, and cyberinfrastructure that enables trustworthy science and NSF's vision of a nation that is a global leader in research and innovation.
- He shared the updated impacts of Trusted CI as of March 2022
  - Impacted over 500 NSF projects since inception in 2012
  - Members of more than 380 NSF projects have attended NSF Cybersecurity Summit
  - Members of more than 250 NSF projects have attended monthly webinars
  - 500 hours of training to the community
  - 64 engagements with NSF funded projects
- Jim shared his view of NSF cyberinfrastructure.
  - Major facilities/large facilities
  - Mid-scale facilities
  - ACCESS Resource Providers
  - Campus Cyberinfrastructure
  - Software & Services (CICI, CSSI, etc.)
  - People & Expertise (CyberTraining)
- He gave some examples of NSF Major Facilities
- He described the JASON Report on Facilities Cybersecurity and the 7 recommendations on risk assessment, strategy coordination, annual reviews, incident response, resourcing, planning, and national security.

    - https://www.nsf.gov/news/special_reports/jasonreportcybersecurity/
    - He said that it's been an important guiding set of recommendations for them over the past year.
- Jim said compliance is an important topic for them. He noted that in most cases, NSF research does not fall under a specific compliance program.
    - He said they coordinate with the Regulated Research Community of Practice (RRCoP) on compliance aspects: https://www.regulatedresearch.org/
- He said NSF's approach allows NSF projects the flexibility to shape their cybersecurity program to best support their science mission.
- Jim said the mission of an NSF facility or project is different from the mission of a bank or a hospital.
    - Availability and data integrity are key aspects for the cyberinfrastructure
    - Confidentiality is what's important for a bank or hospital
- Jim said the trusted CI framework establishes best cybersecurity practices for cybersecurity programs
- Jim said as part of their framework offerings.
    - Framework implementation guide for research cyberinfrastructure operators
        - Gives research organizations a community-tailored head start on choosing among good paths and avoiding treacherous ones.
- He shared some of the framework adopters, including FABRIC, GAGE, LIGO, NOIRLab, NRAO, NSO, OOI, and Research
- Jim said that a key aspect of developing a cybersecurity program is to understand your risks. Open science cyber risk profile (OSCRP) is a resource that they've been maintaining over the years to help NSF projects understand and address their risks.
- Jim said that Trusted CI is collaborating with Michigan State University office of the CIO to document the impact of ransomware attack on research.
    - Report available at: hdl.handle.net/2022/26638
- He said software assurance is another focus area for Trusted CI. They have been growing our instructional materials around software security, including some new exercises and materials developed over the past year.
    - 2021 Annual Challenge
    - Software Secure Training
    - In-depth vulnerability assessment
    - Ransomware
- Jim said this past year, they've had a partnership with EPOC, U of Arkansas / DART on science DMZ focused engagement
- Jim mentioned the operational technology in their facilities (telescopes and ships and sensors) and said that the security of that OT is very important to the trusted CI program.
- He discussed a year-long study on the security of operational technology with a focus on the OT that's deployed currently at the NSF major facilities that they've published. He shared some of those findings.
    - Security is a missing element for OT procurement requirements
    - Organizational "siloing" between IT security personnel and OT operators

    - Some host institutions can help MFs with IT/OT security but even they may not have OT security expertise appropriate to instruments in MFs
    - Newer OT contains exactly the same vulnerabilities as traditional IT systems
- Jim discussed the Trusted CI fellows program and webinars as well as the annual NSF cybersecurity summit (October 2023 in Berkeley, CA)
- Jim said their partnership with CI Compass was very important to them. He said it is a good partner because often the cybersecurity depends on good IT management and good systems management. When they are working with a facility, there is often challenges that CI Compass can come in and help them with as they are implementing the cybersecurity program.
- Jim told the group to stay connected with Trusted CI. Email: info@trustedci.org

Questions

- Miron Livny asked about Jim's assessment on software assurance. He said that he's a bit of a pessimist.
    - Jim said he's an optimist on this topic. He said they don't see a lot of security incidents specifically caused by their custom scientific software used in their cyberinfrastructure. Many of their security incidents impacting software are due to the dependencies on more commodity software. He said understanding the dependencies that we have on different pieces of software and what security vulnerabilities that might bring along is key.
    - Jim also said they've had positive interactions with science gateway developers on their interest in providing a secure service as well as some widely used software providers like the Jupyter community.
- Jay Park said different users and different agency applications require a different level of trust. He said he knows that Jim has served the NSF science community quite well but was wondering if he had a plan to extend that to other agencies' applications or other commercial applications.
    - Jim said they remain focused on NSF science, but the partnerships with other security organizations addressing science challenges in other communities are really important to them.

Roundtable

Next Meeting December 7