The NSF Cybersecurity Center of Excellence: Large Facilities Services

James A. Marsteller, Chief Information Security Officer, Pittsburgh Supercomputing Center, NSF CCoE Co-PI.
Von Welch, Director, Center for Applied Cybersecurity Research, Indiana University, NSF CCoE PI,

June 19, 2017

Overview of the NSF CCoE

The genesis of the NSF Cybersecurity Center of Excellence (trustedci.org) is with a series of two workshops, the Scientific Software Security Innovation Institute (S3I2) workshops. The S3I2 workshops, held in 2010 [1] and 2011 [2], included representatives of 35 major NSF-funded projects. The original goal of the workshops was to explore a software institute focused on IT security for the NSF community. What the workshops found is that the NSF community faces strong challenges in obtaining access to IT security expertise. Projects are forced to divert their resources to develop that expertise, address risks haphazardly, unknowingly reinvent basic cybersecurity solutions, and struggle with interoperability. The workshops further determined the need for access to expertise was more critical than any new software product.

In 2012, based on these workshop findings, the NSF funded the Center for Trustworthy Scientific Cyberinfrastructure (CTSC) to provide security expertise to the NSF community. Building on the success of CTSC, the NSF Cybersecurity Center of Excellence (CCoE) was funded in 2016 as an expansion of the CTSC. The CCoE draws is a collaboration of four internationally recognized institutions: Indiana University, the University of Illinois, the University of Wisconsin-Madison, and the Pittsburgh Supercomputing Center.

CCoE Services in support of Large Facilities

Science projects manage a number of risks to their scientific missions including risks typically managed by cybersecurity, i.e. malicious entities who attack IT infrastructure to further their own ends at the expense of legitimate users or to explicitly harm those users. To be effective cybersecurity must be tailored for the science community, taking the community's risks, tolerances, and technologies into account. The CCoE's mission is to provide the NSF Large Facility community expertise in cybersecurity for science This mission is accomplished through one-on-one engagements with projects to address their specific challenges; education, outreach, and training to raise the state of security practice across the scientific enterprise; and leadership in advancing the overall state of knowledge on cybersecurity for science through applied research and community building. Examples of these mechanisms follow. Details can be found on trustedci.org.

One-on-one engagements:

- DKIST: DKIST and the CCoE collaborated to develop a cybersecurity planning guide for DKIST that addresses these terms and conditions, aligns with existing institutional

policies, and can be implemented within DKIST's budgetary limitations. This guide was made generally available for other NSF large facilities and projects [3].

- LIGO: The CCoE, LIGO and the Open Science Grid collaborated to establish an international identity federation in support of LIGO's scientific mission.
- Icecube, LSST, NEON: The CCoE helped with the development, assessment, and improvement of operational cybersecurity programs.
- Globus, Pegasus, OSG: The CCoE provided software security consulting and assurance evaluation to helping the NSF community develop more secure software and assess software they are using (or considering using).

Education, outreach and training:

- Situational awareness: The CCoE provides situational awareness of the current cyber threats to the research and education environment, including those that impact scientific instruments, by providing timely email notifications about relevant software vulnerabilities.
- Webinars: The CCoE offers a monthly webinar series to allow NSF projects to share findings and experiences with each other.
- Training: The CCoE regularly provides training, tailored to the science community, on a number on a number of topics, including log analysis, incident response, federated identity management, and developing a cybersecurity program.

Advancing the state of knowledge through applied research and community building:

- Large Facility Security Working Group: to develop a working relationship between those responsible for cybersecurity across the LFs and to advance the development and implementation of best practices, standards and requirements within the community.
- NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure:The CCoE organizes this annual event to bring together leaders in NSF cyberinfrastructure and cybersecurity to build a trusting, collaborative community, and to address that community's core cybersecurity challenges.

References

[1] William Barnett, Jim Basney, Randy Butler, and Doug Pearson, "Report on the NSF Workshop on Scientific Software Security Innovation Institute (S3I2) (2010)," Oct. 2010 [Online]. Available: https://security.ncsa.illinois.edu/s3i2/s3i2-workshop-final-report.pdf

[2] William Barnett, Jim Basney, Randy Butler, and Doug Pearson, "Report of NSF Workshop Series on Scientific Software Security Innovation Institute (S3I2) (2011)," Oct. 2010 [Online]. Available: https://security.ncsa.illinois.edu/s3i2/S3I2WorkshopReport2011Final.pdf

[3] Jim Marsteller, Craig Jackson, Susan Sons, Jared Allar, Terry Fleury, Patrick Duda, "Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects, v1," Center for Trustworthy Scientific Cyberinfrastructure, Aug. 2014 [Online]. Available: https://scholarworks.iu.edu/dspace/handle/2022/20026. [Accessed: 18-Jun-2017]