Afternoon Session Cybersecurity at Major Facilities
2:00pm – 3:30pm

LARGE FACILITIES WORKSHOP

2021 WEBINAR SERIES

OCTOBER 14, 2021

National
Science
Foundation

Afternoon Session: Cybersecurity at Major Facilities
2:00pm – 3:30pm

Protecting Research from Foreign Influence, Espionage, and Intellectual Property Theft:

Scott McGaunn, FBI Special Agent

Agent McGaunn will discuss the FBI's counterintelligence efforts against America's adversaries, evolving security challenges/threats, the nature of espionage as it relates to the theft of intellectual property at major facilities, research infrastructure and research institutes, and the challenges of illegitimate transfer of technologies.

Afternoon Session: Cybersecurity at Major Facilities 2:00pm – 3:30pm

Panel Discussion on Cybersecurity at Major Research Infrastructures:

- **Panel includes**
- Moderator: **Manish Parashar**, Director, Office of Advanced Cyberinfrastructure, NSF
- **Jim Ulvestad**, Senior Advisor for Research Security, NSF
- **Benjamin Brown**, Director of Facilities Division, Office of Advanced Scientific Computing Research, DOE
- **Mike Witt**, Associate Chief Information Officer for Cybersecurity & Privacy and Senior Agency Information Security Officer, NASA
- **Robert Beverly**, Program Director, Office of Advanced Cyberinfrastructure, NSF

Cybersecurity Panel background

Moderator: Manish Parashar, Director, Office of Advanced Cyberinfrastructure, NSF

- The Office of Advanced Cyberinfrastructure (OAC) supports and coordinates the development, acquisition, and provision of state-of-the-art cyberinfrastructure resources, tools and services essential to the advancement and transformation of science and engineering.
- OAC also supports forward-looking research and education to expand the future capabilities of cyberinfrastructure specific to science and engineering. By fostering a vibrant ecosystem of technologies and a skilled workforce of developers, researchers, staff and users, OAC serves the growing community of scientists and engineers, across all disciplines, whose work relies on the power of an advanced research cyberinfrastructure.

OAC is within the Directorate for Computer and Information Science and Engineering (CISE)

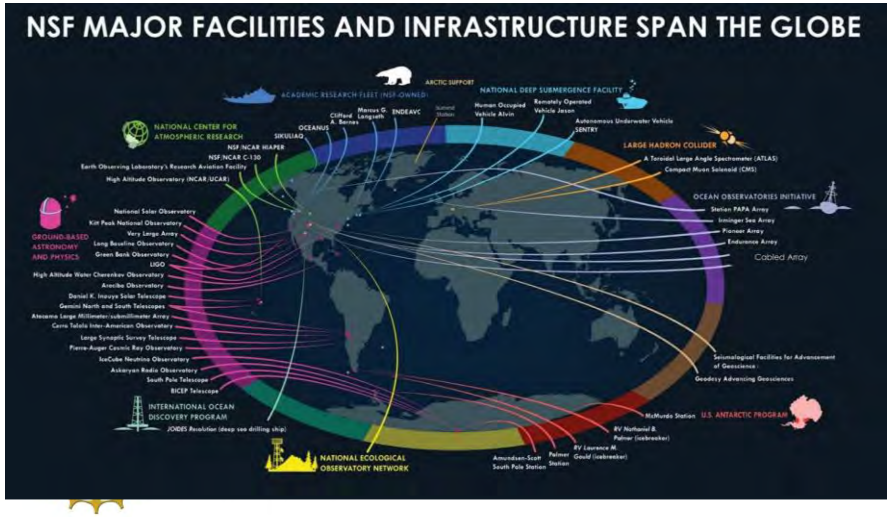
Afternoon Session: Cybersecurity at Major Facilities
2:00pm – 3:30pm

Panel Discussion on Cybersecurity at Major Research Infrastructures:

- Cyberinfrastructure (CI), comprising computing, data, software, and networking and related expertise are critical components of most major research infrastructure and essential to their operations, equitable use, and overall impact. As a result, addressing the growing cybersecurity concerns is essential to ensuring the secure and robust operation of these facilities.
- This session will include a panel and audience discussion on these cybersecurity challenges at major research infrastructure in the 21st century and explore existing best practices and emerging solutions.

Jim Ulvestad, Senior Advisor for Research Security, National Science Foundation

- Until a few days ago, Jim Ulvestad served as NSF’s first Chief Officer for Research Facilities (CORF). The CORF has overall responsibility, on behalf of the NSF Director, for the agency's oversight of major and mid-scale research facilities throughout their lifecycle.
- Previously, Jim served as NSF acting assistant director for Mathematical and Physical Sciences (MPS), leading a directorate that supports research at scales ranging from subatomic particles to the Milky Way galaxy and the universe. Prior to that, he led MPS' Division of Astronomical Sciences from 2010 to 2017.


NSF MAJOR FACILITIES AND INFRASTRUCTURE SPAN THE GLOBE
ARCTIC SUPPORT
ACADEMIC RESEARCH FLEET (NSF-OWNED)
NATIONAL DEEP SUBMERGENCE FACILITY
Clifford A. Barnes
Marcus G. Langseth
ENDEAVC
Summit Station
Human Occupied Vehicle Alvin
Remotely Operated Vehicle Jason
Autonomous Underwater Vehicle SENTRY
OCEANUS
SIKULIAQ
NATIONAL CENTER FOR ATMOSPHERIC RESEARCH
NSF/NCAR HIAPER
NSF/NCAR C-130
Earth Observing Laboratory's Research Aviation Facility
High Altitude Observatory (NCAR/UCAR)
LARGE HADRON COLLIDER
A Toroidal Large Angle Spectrometer (ATLAS)
Compact Muon Solenoid (CMS)
OCEAN OBSERVATORIES INITIATIVE
Station PAPA Array
Irminger Sea Array
Pioneer Array
Endurance Array
Cabled Array
GROUND-BASED ASTRONOMY AND PHYSICS
National Solar Observatory
Kitt Peak National Observatory
Very Large Array
Long Baseline Observatory
Green Bank Observatory
LIGO
High Altitude Water Cherenkov Observatory
Arecibo Observatory
Daniel K. Inouye Solar Telescope
Gemini North and South Telescopes
Atacama Large Millimeter/submillimeter Array
Cerro Tololo Inter-American Observatory
Large Synoptic Survey Telescope
Pierre-Auger Cosmic Ray Observatory
IceCube Neutrino Observatory
Askaryan Radio Observatory
South Pole Telescope
BICEP Telescope
Seismological Facilities for Advancement of Geoscience
Geodesy Advancing Geosciences
INTERNATIONAL OCEAN DISCOVERY PROGRAM
JOIDES Resolution (deep sea drilling ship)
McMurdo Station
U.S. ANTARCTIC PROGRAM
RV Nathaniel B. Palmer (icebreaker)
RV Laurence M. Gould (icebreaker)
Palmer Station
Amundsen-Scott South Pole Station
NATIONAL ECOLOGICAL OBSERVATORY NETWORK

- “NSF’s facilities have unique scientific data and capabilities, and thus are interesting targets for cybercriminals who want to steal intellectual property or disrupt activities at high-profile targets”

U.S. DEPARTMENT OF ENERGY | Office of Science

Benjamin Brown, Ph.D., Director of Facilities Division
Office of Advanced Scientific Computing Research (ASCR)
Department of Energy

- Ben Brown leads ASCR’s Facilities Division, which conceives, constructs, and operates world-leading open access supercomputing, data, and networking facilities to enable the DOE mission and the national research enterprise.
- The Division’s $575M annual budget supports High Performance Computing and Leadership Computing Facilities at Lawrence Berkeley, Oak Ridge, and Argonne National Laboratories; and the Energy Sciences Network (ESnet), which delivers high performance data transport capabilities for large-scale science.
- From 2014-21 Ben was the founding program manager for the Department’s Project Leadership Institute, which is devoted to training the next generation of DOE project leaders.
- Prior to joining the DOE in 2008, Ben conducted research on optical control of quantum systems and quantum information science, and served as a AAAS Congressional Fellow at the U.S. Senate.
- He holds a bachelor’s degree in physics from Harvard University and a Ph.D. in optics from the University of Rochester.

Mike Witt, Associate Chief Information Officer for Cybersecurity & Privacy and Senior Agency Information Security Officer, NASA

- Mike Witt is NASA's Associate Chief Information Officer (ACIO) for Cybersecurity & Privacy and Senior Agency Information Security Officer (SAISO). He joined the agency in 2017 as the Deputy SAISO.

- Before NASA, he served with the Department of Homeland Security (DHS) supporting the Director of the National Cybersecurity & Communications Integration Center and the Director of Network Security Deployment to enhance existing EINSTEIN 3 - Accelerated (E3A) technology and cyber detection/response operational capabilities.

- Prior to DHS, he held multiple roles at the Internal Revenue Service (IRS) including Director, Computer Security Incident Response Center, where he was responsible for the agency's incident handling, analysis, and vulnerability management. While there, he created an Emerging Threats Team to provide advanced analysis, analytics, network forensics, and cyber threat intelligence capabilities.

National Science Foundation

Robert Beverly, Program Director, Office of Advanced Cyberinfrastructure, National Science Foundation

- Rob Beverly is a Program Officer in NSF's Office of Advanced Cyberinfrastructure and an Associate Professor of Computer Science at the Naval Postgraduate School in Monterey, CA.

- His work focuses on applied system and network security. He created the spoofer project, co-authored RFC8567, and research from his lab has improved the robustness of widely deployed Internet protocols including IPv6, TCP, and BGP. Rob has helped chair ACM IMC, SOSR, Hotnets, PAM, and DFRWS, and will be speaking at Blackhat this summer.

- Prior to academia, he was a network scientist with BBN and a network engineer at MCI. Dr. Beverly holds an undergraduate degree from Georgia Tech and a PhD from MIT.

OAC is within the Directorate for Computer and Information Science and Engineering (CISE)

Afternoon Session: Cybersecurity at Major Facilities
2:00pm – 3:30pm

Panel Discussion on Cybersecurity at Major Research Infrastructures:

1. What are the unique cybersecurity challenges related to large facilities at your agency?
2. Do you see a tensions between enforcing cybersecurity and the usability and performance of your facilities? Is so, how do you manage this tension? What are the effective tradeoffs that you have implemented?
3. Developing/attracting and retaining a diverse and skilled CI workforce is a crosscutting challenge. What are specific challenges in cybersecurity, and how are you addressing these challenges?
4. Are there unique threats/attack vectors (e.g., internal threats / insider attacks) that large facilities should be concerned about? How do you manage such threats/ attack vectors?

Afternoon Session: Cybersecurity at Major Facilities 2:00pm – 3:30pm

Panel Discussion on Cybersecurity at Major Research Infrastructures:

5. Recognizing the increase of ransomware attacks overall, what is the implication of such an attack on a large facility? Could a large facility recover from such an attack, given the volumes of research data / artifacts?
6. What is the role of CoTS security solutions in implement cybersecurity for large facilities? Do they work, and where are they not sufficient?
7. Would large facilities benefit from red-teaming exercises? Is there an inter-agency role for such exercises?

Afternoon Session: Cybersecurity at Major Facilities
2:00pm – 3:30pm

Panel Discussion on Cybersecurity at Major Research Infrastructures:

8. How can large facilities protect the integrity of research data / artifacts? What role can emerging private data sharing techniques (differential privacy, homomorphic encryption, etc.) play in improving the security/robustness of large facilities?

9. Rank the following CI cybersecurity concerns and discuss the motivation for your ranking: availability, data loss, reputation.

Afternoon Session: Cybersecurity at Major Facilities 2:00pm – 3:30pm

Panel Discussion on Cybersecurity at Major Research Infrastructures:

Many thanks to all of today's participants

If you have a question that cannot be answered during this panel discussion, please email it to LFWorkshop@nsf.gov.