

Strengthening Trustworthy Science: Ideas for Adapting the NIST Risk Management Framework to the NSF Cooperative Agreement for Large Facilities

2016 NSF Cybersecurity Summit
for Large Facilities and Cyberinfrastructure
August 18, 2016

Tim Howard, CISSP
Division of Polar Programs
GeoSciences Directorate
National Science Foundation

With Appreciation and Thanks to Steve Baret,
IceCube Neutrino Observatory
University of Wisconsin

The views expressed here are entirely my own and do not represent the National Science Foundation or any other agency, organization, or person mentioned herein.



BLUF: Compliance is Imminent... Resistance is Futile...
So Embrace It...



A Quiz: Raise your hand if...

- You were here last year.
- You are using, or at least familiar with, Project Management and/or the PMBOK to manage your activities.
- Your program or project is on the NSF Large Facility List.
- You are managing your project using the NSF CA-FATC and LF Manual.
 - By the way, for some of you, your G/AO is in the audience...



Science Facility: Scott's Hut at Cape Evans, Ross Island, 1910



If you were here last year...

- “Compliance is Imminent... So embrace it...”
 - Anurag Shanker, Indiana University
 - Good Primer on HIPAA, FISMA, NIST Risk Management Framework (RMF)
- Lighter than NIST, heavier than small business guidelines
 - Developing Cybersecurity Programs for NSF Projects (Training by Cowles, Jackson, Marsteller, Sons)
 - Also references to cybersecurity in NSF Cooperative Agreement terms & conditions
 - Good training on how to get a program started.
- “Why don’t you (NSF) tell us what to do? Cliff Jacobs, NSF (Retired)

Compliance is Imminent

- Biomedical research is on a collision course with research CI.
- With little biomedical research CI around, an increasingly larger volume of ePHI can be expected to land on our systems.
- Grants and contracts will be asking for FISMA compliance.
- ... So embrace it.

How is the guide different?

1. Authored with a **CI perspective**
2. Contributions and critique from LF/CI community (TrustedCI Forum, DKIST)
3. Lighter than FISMA/NIST SPs
4. Heavier than, *e.g.*, FCC’s small business policy creation tool or NISTIR 7621 *Small Business Information Security: The Fundamentals*
5. **Publicly** available and **free** to use (unlike, *e.g.*, ISO)
6. **Templates, templates, templates!!!**
7. Community-driven approach - **Community to contribute** to the evolution of the guide



Summit 2015 Outcome: What We Want...

1. Broadly applicable strategy for security budgets;
2. Security spending metrics to drive balance with science mission;
3. The correct accountability, risk responsibility, and risk acceptance practices, implemented correctly (Effective & Efficient);
4. Community requirements for software assurance, quality, and supply chain;
5. Common, broadly applicable information security framework;
6. Common risk-based cybersecurity approaches that address unique science needs;
7. Collaboratively developed cybersecurity programs;
8. Identity and access management best practices to support research;
9. Privacy & CI cybersecurity baseline within the context of science mission;
10. More NSF grant money for basic and applied cybersecurity research;
11. Community threat model to improve our collective cybersecurity risk management;
12. Improve existing cross-organizational mechanisms to gain a defensive advantage;

Source: 2015 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure final report



Summit 2015 Outcome: Your Tax Dollars At Work...

- SP 800-18: Guide for Developing **Security Plans** for Federal Information Systems
- SP 800-28: Guidelines on **Active Content and Mobile Code**
- SP 800-30: Guide for Conducting **Risk Assessments**
- SP 800-34: **Contingency Planning** Guide for Federal Information Systems
- SP 800-37: Guide for Applying the **Risk Management Framework** to Federal Information Systems: a Security Life Cycle Approach
- SP 800-39: **Managing Information Security Risk: Organization, Mission, and Information System View**
- SP 800-46: Guide to **Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security**
- SP 800-47: Security Guide for **Interconnecting Information Technology** Systems
- SP 800-53: **Security and Privacy Controls** for Federal Information Systems and Organizations
- SP 800-55: **Performance Measurement Guide** for Information Security
- SP 800-60: Guide for Mapping Types of **Information and Information Systems** to Security Categories
- SP 800-61: **Computer Security Incident Handling Guide**
- SP 800-63-2: **Electronic Authentication Guideline**
- SP 800-64: Security Considerations in the **System Development Life Cycle**
- SP 800-65: Integrating IT Security into the **Capital Planning and Investment Control Process**
- SP 800-82: Guide to **Industrial Control Systems (ICS) Security**
- SP 800-100: Information Security Handbook: A Guide for Managers
- SP 800-122: Guide to Protecting the Confidentiality of **Personally Identifiable Information (PII)**
- SP 800-144: Guidelines on **Security and Privacy in Public Cloud Computing**
- SP 800-161: **Supply Chain Risk Management Practices** for Federal Information Systems and Organizations
- SP 800-163: Vetting the Security of **Mobile Applications**

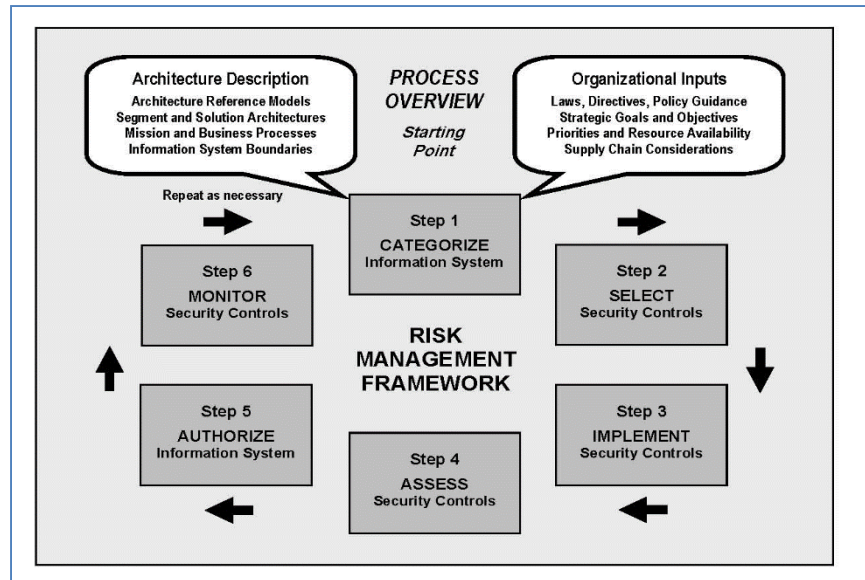


My Focus for Today

2015 Summit Recommendations:

- 3. The correct accountability, risk responsibility, and risk acceptance practices, implemented correctly (Effective & Efficient);
- 5. Common, broadly applicable information security framework;
- 6. Common risk-based cybersecurity approaches that address unique science needs;
- 7. Collaboratively developed cybersecurity programs;

IceCube Neutrino Observatory as a “case study;” Thanks to ICNO!



CTSC Cybersecurity Program Processes & Core Tools







Early Science "Cyber" Infrastructure in the U.S. Thomas Jefferson – Weather Bug, c. 1776

| 4 th of July readings: | |
|-----------------------------------|-------------------|
| Hr | Temp |
| 6- 0 am | 68. |
| 9- 0 | 72 ^{1/4} |
| 1- 0 pm | 76. |
| 9- 0 | 73 ^{1/2} |

Source: memory.loc.gov

- Jefferson's "iPad" with manual uplink to his "desktop" ledgers (standard IT)
- Continual observations on 2 continents for over 40 years (instruments)
- Recruited volunteer observers (sensors) at any opportunity
- Instructions to Lewis & Clark included climate and weather observations



Source: <http://www.loc.gov/exhibits/jefferson/images/vc65.jpg>
 Source: "Weather observations," http://wiki.monticello.org/mediawiki/index.php/Weather_Observations (2007)
 "Weather observations in early American history," http://celebrating200years.noaa.gov/foundations/weather_obs/welcome.html#earlyyear (2007)

1911: Early Science in Antarctica



Scott's Hut at Cape Evans, c. 1911

1911: Early Science Cyberinfrastructure in Antarctica



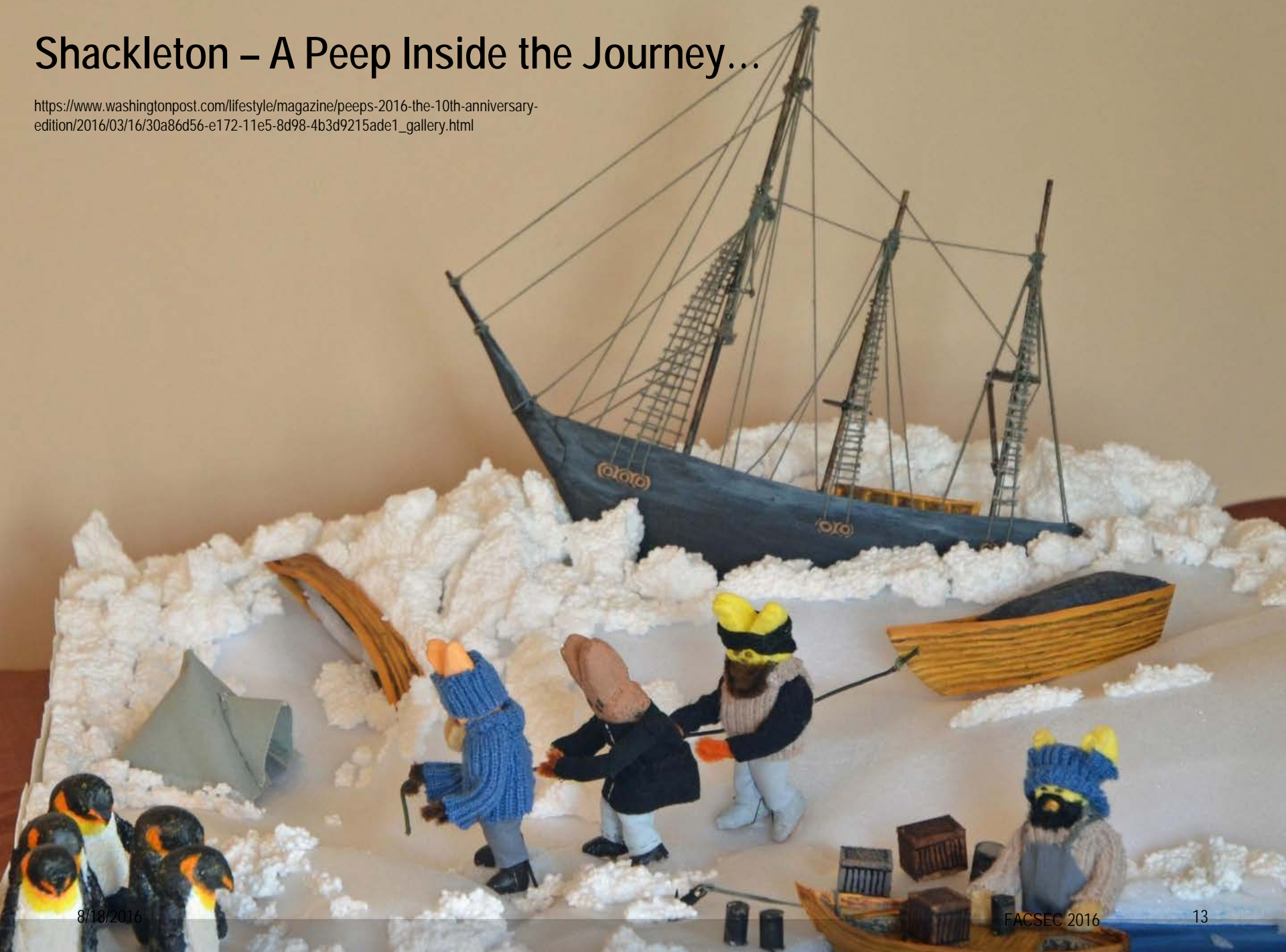
Scott's Hut at Cape Evans, c. 1911

1914 – 1916: HMS Endurance

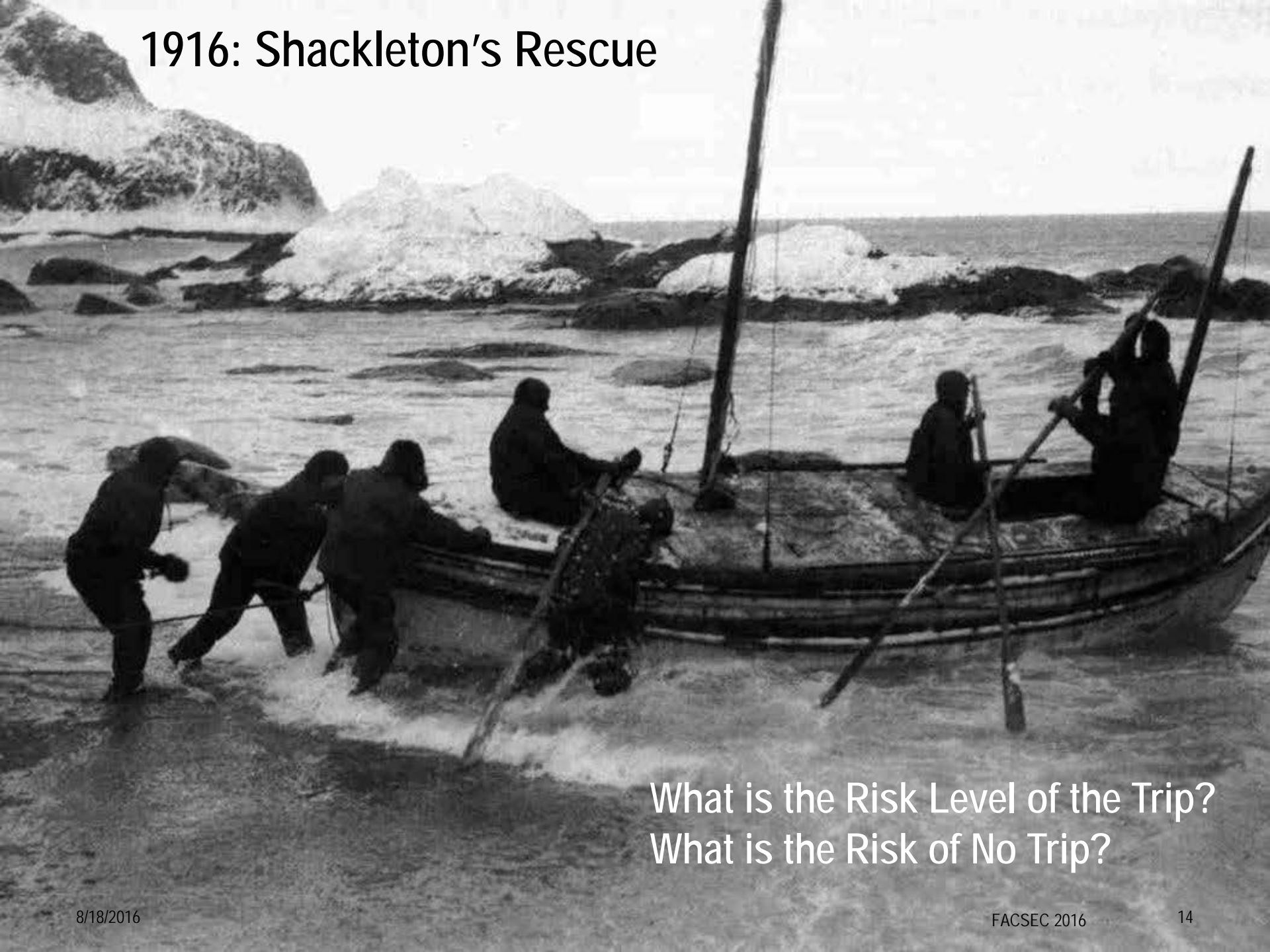


Shackleton – A Peep Inside the Journey...

https://www.washingtonpost.com/lifestyle/magazine/peeps-2016-the-10th-anniversary-edition/2016/03/16/30a86d56-e172-11e5-8d98-4b3d9215ade1_gallery.html



1916: Shackleton's Rescue



What is the Risk Level of the Trip?
What is the Risk of No Trip?

2016: Antarctic Science Today

- Astrophysics and Geospace Sciences
- Organisms and Ecosystems
- Integrated System Science
- Antarctic Instrumentation and Technology Development
- Earth Sciences
- Glaciology
- Ocean and Atmospheric Sciences
- Technical Events
- Artist and Writers Program

SPICECORE Project
South Pole, 2016

Amundsen-Scott South Pole Station



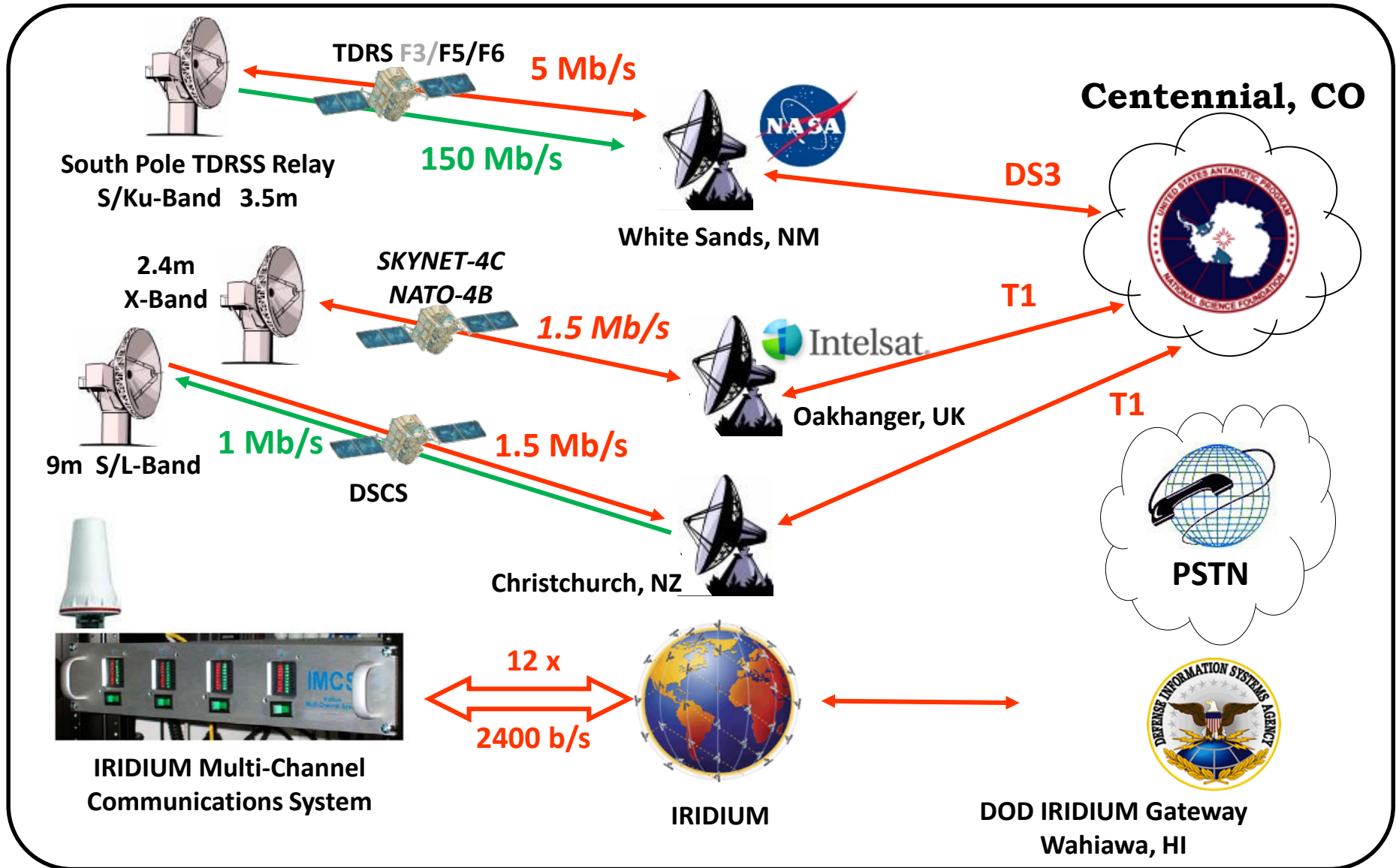
2016: Antarctic Science Cyberinfrastructure Today



SATCOM RADOME, South Pole, 2016

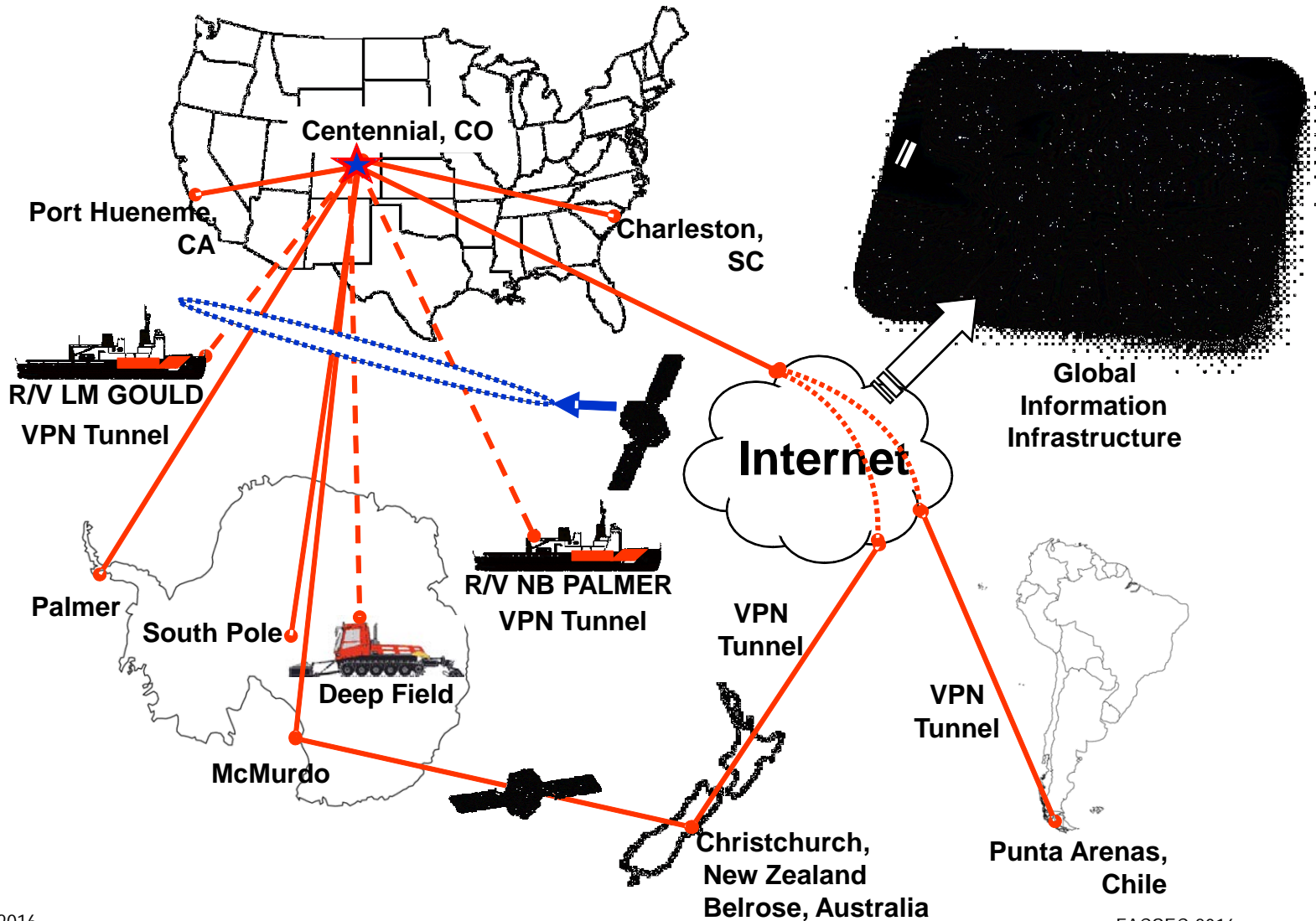


South Pole Station Satellite Networking





USAP Science & Operations CyberInfrastructure





USAP CyberInfrastructure at a Glance

Voice/Telephony

- 3 PBXs with 2,000+ subscriber ports
- Global, enterprise VoIP system w/500+ phones
- ~ 149 IRIDIUM ISU mobile phones with > \$900K in annual mobile satellite air time

Data Systems

- ~ 300 servers, enterprise-wide
- Network File Storage:
 - Centennial, CO: 2.5 Terabytes
 - McMurdo: 7 Terabytes
 - South Pole: 2 Terabytes
 - Research Vessels: 1.5 Terabytes
- 3,800+ enterprise e-mail addresses
- 100,000 to 115,000 e-mail messages to/from enterprise mail servers
- Up 200+ GBytes of data transferred daily from South Pole

USAP Enterprise Network

- Backbone for program communications
- Centrally supported from Centennial, CO
- Converged Service - Voice, Video, Data
- Commodity Internet Service
- 7 inter-site network links via satellite (both conventional commercial and non-standard)

Network

- ~ 290+ managed devices
- ~ 2,800 total ports

Global Reach

- 11 total operating locations
- 2 research vessels
- 3 Antarctic Stations

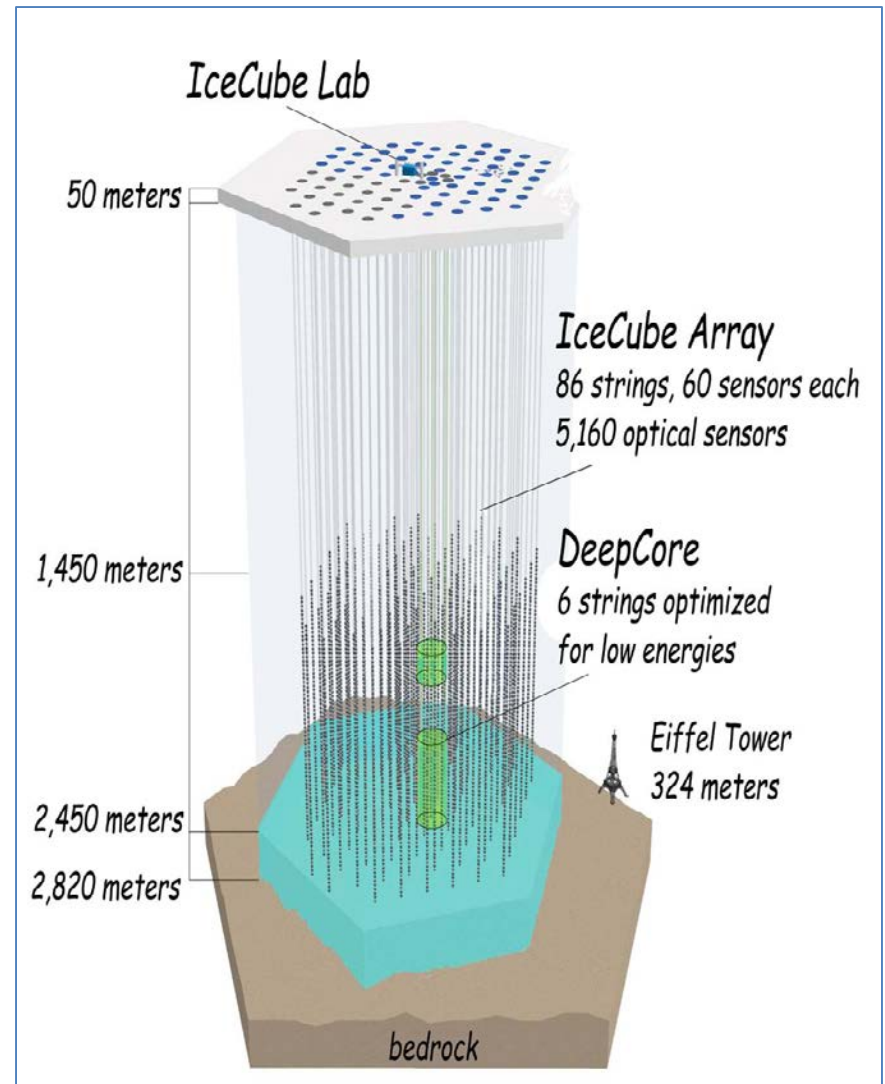
Modern Science in Antarctica: IceCube Neutrino Observatory





Modern Science in Antarctica: IceCube Neutrino Observatory

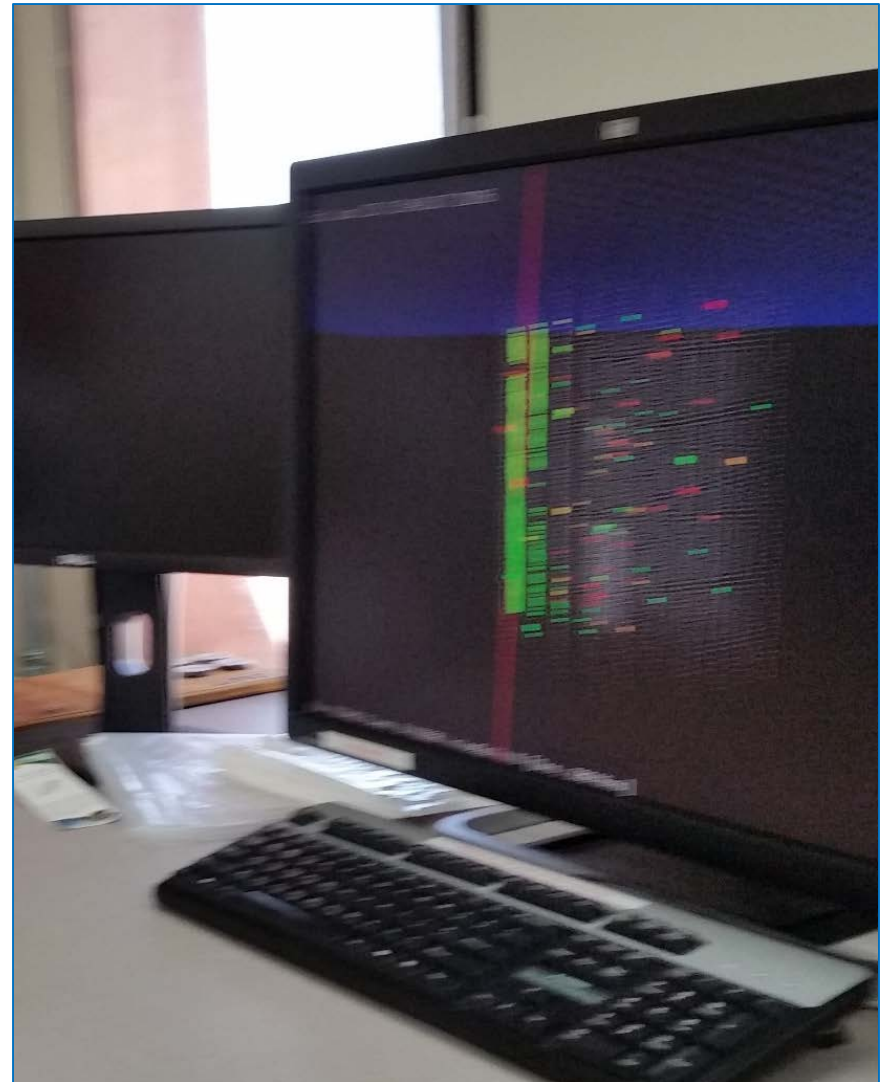
- World's largest neutrino detector, encompassing a cubic kilometer of ice.
- Designed to detect particles from cataclysmic events that have energies a million times greater than nuclear reactions.
- IceCube detects 275 atmospheric neutrinos daily and ~100,000 per year.
- 300 scientists at 47 institutions in 12 countries conduct IceCube science.
- Total cost \$279 million USD; NSF provided \$242 million for construction
- In 2013, IceCube reported first detection of high-energy cosmic neutrinos, opening a new astronomical vista on the universe and on some of its most violent phenomena.
- In March 2016, NSF renewed Operations & Maintenance agreement for five years, total cost \$35 million.





IceCube Neutrino Observatory Cyberinfrastructure

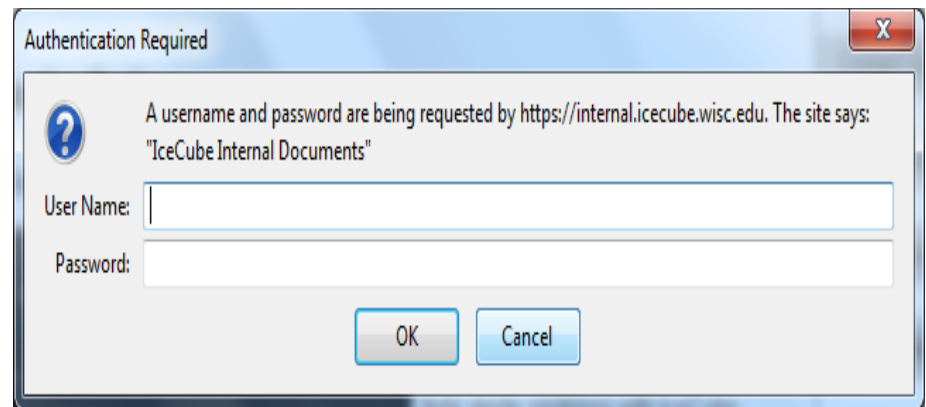
- Data acquisition maintenance and computing infrastructure;
- Long-term data archive;
- Simulation production and data acquisition firmware support;
- Maintenance of IceTop (surface);
- Software, including online filtering and simulation;
- Calibration efforts;
- Reconstruction and analysis tools;
- Simulation software and production;
- Education and outreach program;
- Data centers preserve a second copy of raw data;
- Simulation production is international distributed effort.





IceCube Neutrino Observatory CyberSecurity

- 2013 CTSC Engagement
- 2014 Incident (CTSC report)
- 2016 System Security Plan
- University of Wisconsin, as primary grantee, owns CyberSecurity; policies, etc.
- International Collaboration partners contribute to cybersecurity success

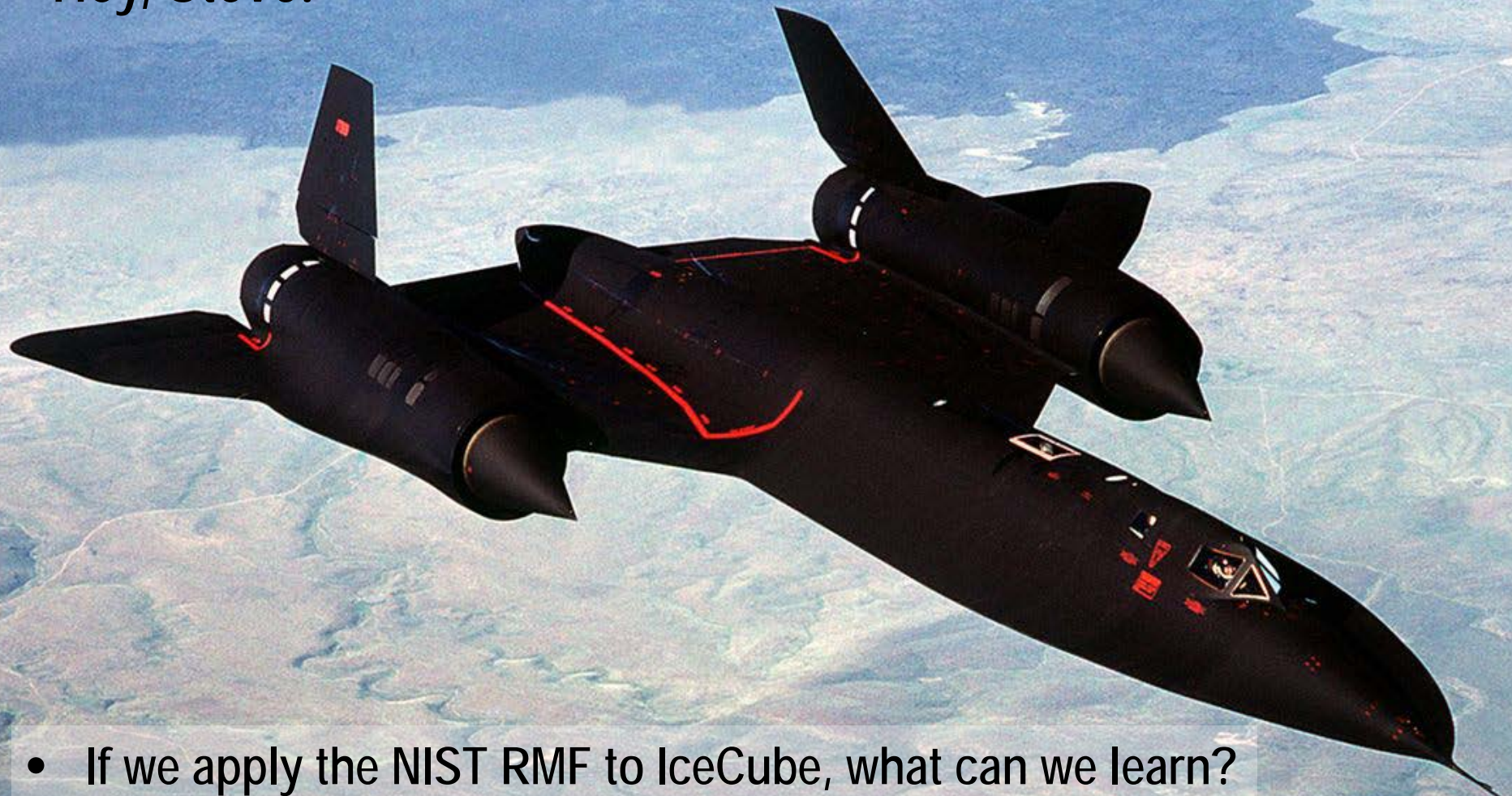




USAP & IceCube – Why Do We Care?

- Why do we need to care about IceCube information security?
- Simple Answer: **We interconnect.** IceCube uses USAP infrastructure for its mission.
- This represents a potential path for a malicious actor to gain access into USAP OR University of Wisconsin/IceCube partners.
- How do I determine if the interconnection is secure?
- Trust and Verify
- Verify What? Verify How? What are the standards of trust that apply?
- **Does FISMA apply to IceCube? (*Compliance is Imminent...*)**

“Hey, Steve!”



- If we apply the NIST RMF to IceCube, what can we learn?
- High Altitude, Fast pass across the RMF;
- This is entirely hypothetical;
- Nothing is binding.

Does FISMA Apply Here?



- **Three Possible Answers:**
 - NO, and you cant make me...
 - YES, and you are late...
 - Mebbe, Mebbe Not...
- **Is there a Fourth Answer?**



What is FISMA anyway?

- Federal Information Security Management Act of 2002; updated by the Federal Information Security Modernization Act of 2014; United States Code: 44 USC 3554;
- FISMA assigns the head of each federal agency the responsibility for “providing information security **protections commensurate with the risk and magnitude of the harm** resulting from unauthorized access, use, disclosure, disruption, modification, or destruction” of the **information and information systems that support agency mission and business functions** (44 USC 3554).
- OMB requires agencies “to **employ risk-based approaches and decision making** to ensure that security and privacy capabilities are sufficient to protect agency assets, operations, and individuals.” (Circular A-130, July 2016)
- “Ultimately, **agency heads remain responsible and accountable** for ensuring that information management practices comply with all Federal requirements, that information security and privacy programs are appropriately managed, and that **Federal information is adequately protected** commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information.” (A-130)



What Does FISMA Say?

- FISMA describes Federal agency security responsibilities as including **“information collected or maintained by or on behalf of an agency”** and **“information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.”**
- FISMA requires each agency to **provide information security for the information and “information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.”** This includes services that are either fully or partially provided, including agency-hosted, outsourced, and cloud-based solutions.
- Additionally, because **FISMA** applies to Federal information and information systems, in certain circumstances, **its requirements also apply to** a specific class of IT that the Clinger-Cohen Act of 1996 (40 U.S.C. § 11101(6)) did not include, i.e., **“equipment that is acquired by a Federal contractor incidental to a Federal contract.”** Therefore, when **Federal information** is used within incidentally acquired equipment, the agency continues to be responsible and accountable for ensuring that **FISMA** requirements are met for such information.



What Does OMB Say?

Circular A-130, *Managing Information as a Strategic Resource*, effective July 28, 2016

- Section 10. Definitions;
- 2) 'Adequate security' means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that **information hosted on behalf of an agency** and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.
- 22) 'Federal information' means information created, collected, processed, maintained, disseminated, disclosed, or disposed of **by or for the Federal Government**, in any medium or form.
- 23) 'Federal information system' means an information system used or **operated by** an agency or by a contractor of an agency or by **another organization** on behalf of an agency.
- 48) 'Information technology resources' means all agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, or other activity related to the life cycle of information technology; acquisitions or interagency agreements that include information technology and the services or equipment provided by such acquisitions or interagency agreements;
- **but does not include grants that establish or support information technology not operated directly by the Federal Government.**



Appendix I to OMB Circular A-130: Non-Federal Entities

*Responsibilities for Protecting and Managing Federal Information Resources, Section 4, Specific Requirements, subsection j. **Non-Federal Entities***

- 1) **terms and conditions in contracts and other agreements** involving creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of Federal information, **incorporate security and privacy requirements** and are sufficient to enable agencies to meet Federal and agency-specific requirements pertaining to the protection of Federal information;
- 2) **Provide oversight of information systems used or operated by contractors or other entities on behalf of the Federal Government or that collect or maintain Federal information on behalf of the Federal Government**, to include:
 - 2.a) **Documenting and implementing policies and procedures for information security and privacy oversight**, to include ensuring appropriate vetting and access control processes for contractors and others with access to information systems containing Federal information;
 - 2.b) **Ensuring that security and privacy controls** of such information systems and services are effectively implemented and **comply with NIST standards and guidelines and agency requirements**;
 - 2.c) Ensuring that these information systems are included in the agency's inventory of information systems;



Appendix I to OMB Circular A-130

Non-Federal Entities

Responsibilities for Protecting and Managing Federal Information Resources, Section 4, Specific Requirements, subsection j. Non-Federal Entities

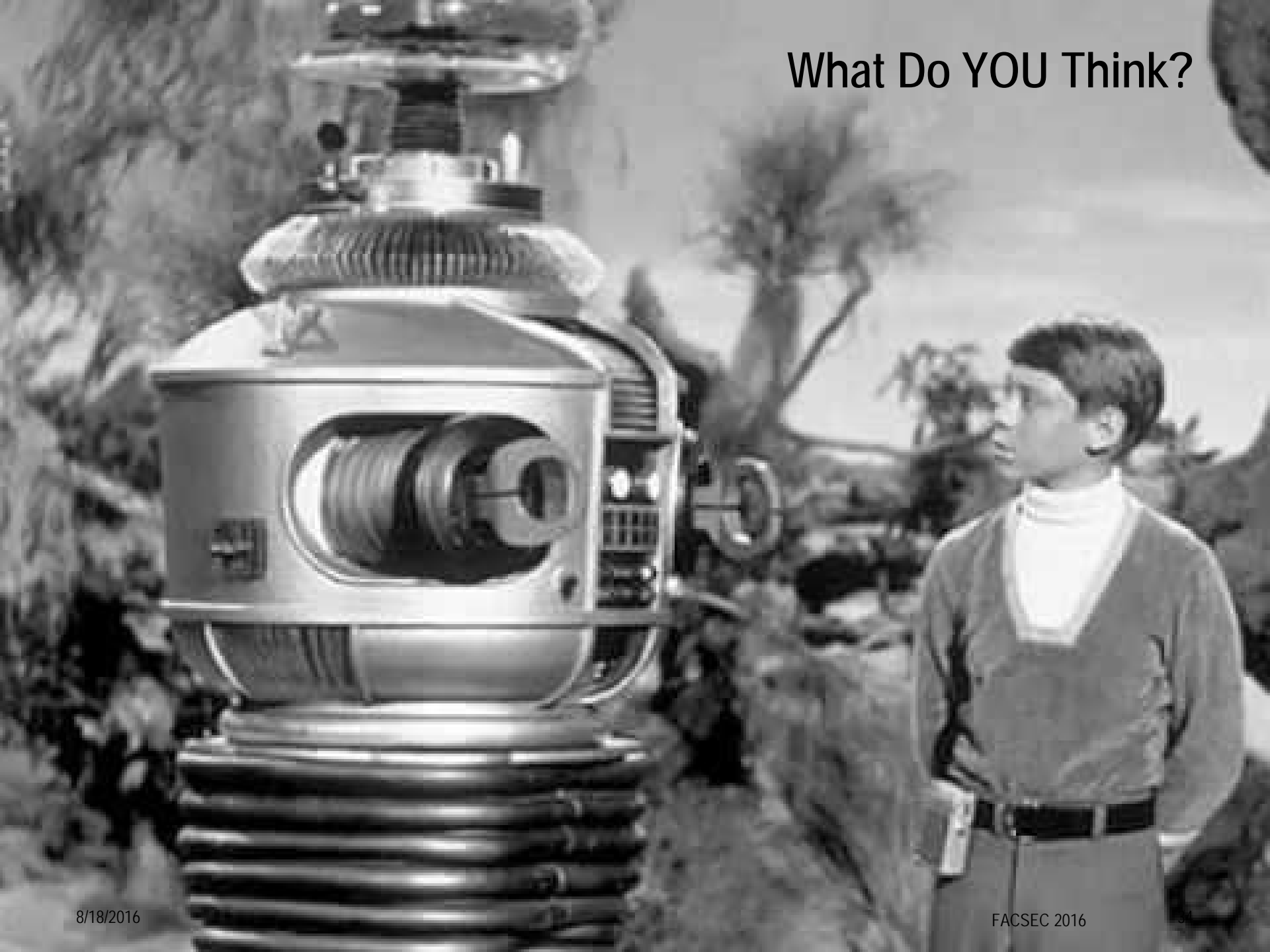
- **2.d) Ensuring that the interface characteristics, security requirements, and the nature of the information communicated is documented for each interface between these systems and agency-owned or operated information systems;**
- 2.e) Ensuring that procedures are in place for incident response for these information systems including timelines for notification of affected individuals and reporting to OMB, DHS, and other entities as required in OMB guidance;
- **2.f) Requiring agreements (e.g., memoranda of understanding, interconnection security agreements, contracts) for interfaces between these information systems and agency-owned or operated information systems; and**
- 3) Consistent with the agency's authority, ensure that the requirements of the Privacy Act apply to a Privacy Act system of records when a contractor operates the system of records on behalf of the agency to accomplish an agency function;
- 4) **Collaborate with non-Federal entities** and other agencies as appropriate to **ensure that security and privacy requirements** pertaining to these non-Federal entities, such as State, local, tribal, and territorial governments, are **consistent to the greatest extent possible**; and
- **5) Ensure that terms and conditions of contracts and other agreements include sufficient provisions for Federal Government notification and access, as well as cooperation with agency personnel and Inspectors General.**



What Does NSF Do About FISMA?

- **FISMA applies to NSF information systems managed by the agency**
 - eJacket
 - iTrak
 - USAP information systems
- **Does FISMA apply to grants issued by NSF to institutions and organizations?**
 - FAR and grants, OMB and grants
- **Does FISMA apply to Cooperative Agreements between NSF and institutions?**
 - CA-FATC
- **How about Large Facilities?**
 - CA-FATC/LF, LFO Manual

What Do YOU Think?



1944: New frontiers of the mind...

-2-

THE WHITE HOUSE

WASHINGTON

November 17, 1944

Dear Dr. Bush:

The Office of Scientific Research and Development, of which you are the Director, represents a unique experiment of team-work and cooperation in coordinating scientific research and in applying existing scientific knowledge to the solution of the technical problems paramount in war. Its work has been conducted in the utmost secrecy and carried on without public recognition of any kind; but its tangible results can be found in the communiques coming in from the battlefronts all over the world. Some day the full story of its achievements can be told.

There is, however, no reason why the lessons to be found in this experiment cannot be profitably employed in times of peace. The information, the techniques, and the research experience developed by the Office of Scientific Research and Development and by the thousands of scientists in the universities and in private industry, should be used in the days of peace ahead for the improvement of the national health, the creation of new enterprises bringing new jobs, and the betterment of the national standard of living.

It is with that objective in mind that I would like to have your recommendations on the following four major points:

First: What can be done, consistent with military security, and with the prior approval of the military authorities, to make known to the world as soon as possible the contributions which have been made during our war effort to scientific knowledge?

The diffusion of such knowledge should help us stimulate new enterprises, provide jobs for our returning servicemen and other workers, and make possible great strides for the improvement of the national well-being.

Second: With particular reference to the war of science against disease, what can be done now to organize a program for continuing in the future the work which has been done in medicine and related sciences?

The fact that the annual deaths in this country from one or two diseases alone are far in excess of the total number of lives lost by us in battle during this war should make us conscious of the duty we owe future generations.

Third: What can the Government do now and in the future to aid research activities by public and private organizations? The proper roles of public and of private research, and their interrelation, should be carefully considered.

Fourth: Can an effective program be proposed for discovering and developing scientific talent in American youth so that the continuing future of scientific research in this country may be assured on a level comparable to what has been done during the war?

New frontiers of the mind are before us, and if they are pioneered with the same vision, boldness, and drive with which we have waged this war we can create a fuller and more fruitful employment and a fuller and more fruitful life.

I hope that, after such consultation as you may deem advisable with your associates and others, you can let me have your considered judgment on these matters as soon as convenient - reporting on each when you are ready, rather than waiting for completion of your studies in all.

Very sincerely yours,

/s/

Franklin D. Roosevelt

Dr. Vannevar Bush,
Office of Scientific Research and Development
Washington, D. C.



1945: Science – The Endless Frontier

- "New frontiers of the mind are before us, and if they are pioneered with the same vision, boldness, and drive with which we have waged this war we can create a fuller and more fruitful employment and a fuller and more fruitful life."
 - FRANKLIN D. ROOSEVELT, November 17, 1944.
- Therefore I recommend that a new agency for these purposes be established. Such an agency should be composed of persons of broad interest and experience, having an understanding of the peculiarities of scientific research and scientific education. It should have stability of funds so that long-range programs may be undertaken. It should recognize that freedom of inquiry must be preserved and **should leave internal control of policy, personnel, and the method and scope of research to the institutions in which it is carried on**. It should be fully responsible to the President and through him to the Congress for its program.
 - Vannevar Bush, Science The Endless Frontier, 1945



Excerpts from the National Science Foundation Act of 1950

§1870. General authority of Foundation

- The Foundation shall have the **authority**, within the limits of available appropriations, **to do all things necessary** to carry out the provisions of this chapter, including, but without being limited thereto, the authority—
 - **(a) to prescribe such rules and regulations as it deems necessary governing the manner of its operations and its organization and personnel;**



“Why Don’t You Tell Us What To Do?”

Guidance to NSF as an Executive Branch Agency

- NSF Act of 1950
- FISMA 2002 and 2014
- FITARA 2015
- United States Code (U.S.C.) and Code of Federal Regulations (CFR)
- Federal Acquisition Regulations (FAR)
- OMB Circular A-130 (2000 and 2016)
- OMB Memoranda
- NIST FIPS & Special Pubs

Guidance for NSF Grants and Cooperative Agreements

- NSF PAPPG (Jan 2016)
- NSF Cooperative Agreement Financial Award Terms & Conditions (CA-FATC) (Jul 2016)
- CA-FATC Supplement for Large Facilities (Jan 2016)
- NSF Large Facility Manual (Jun 2015) (draft update under development)

NSF Advanced CyberInfrastructure (ACI) Research Program

- Center for Trusted Scientific CyberInfrastructure (CTSC) & Summit referenced.



What Does NSF Tell You To Do?

PAPPG, January 2016

- Extracts from Proposal and Award Policies and Procedures Guide (PAPPG)
- Data Management Plan may include: policies for access and sharing including **provisions for appropriate protection of privacy, confidentiality, security, intellectual property, or other rights or requirements;**
- NSF normally **allows grantees to retain principal legal rights to intellectual property developed under NSF grants** to provide incentives for development and dissemination of inventions, software and publications that can enhance their usefulness, accessibility and upkeep. Such incentives do not, however, reduce the responsibility that investigators and organizations have as members of the scientific and engineering community, to make results, data and collections available to other researchers.
- **Data collection activities of NSF grantees are the responsibility of grantees,** and NSF support of a project does not constitute NSF approval of the survey design, questionnaire content or data collection procedures. **No representation may be made to respondents that such data are being collected for, or in association with, NSF or the government.** However, this requirement is not intended to preclude mention of NSF support of the project in response to an inquiry or acknowledgment of such support in any publication of this data (see AAG Chapter VI.E.4).



What Does NSF Tell You To Do? CA-FATC, July 2016

- Cooperative Agreement Financial & Administrative Terms and Conditions
- 1. Awardee Responsibilities and Compliance with Federal Requirements
- 1.a. The **awardee has full responsibility for the conduct of the project or activity supported under this award and for adherence to the award conditions**. Although the awardee is encouraged to seek the advice and opinion of NSF on special problems that may arise, such advice does not diminish the awardee's responsibility for making sound scientific and administrative judgments and should not imply that the responsibility for operating decisions has shifted to NSF.
- 1.b. The **requirements of this award are contained in these Cooperative Agreement Financial & Administrative Terms and Conditions unless otherwise specified in the notice of award**. The applicable Federal administrative standards are incorporated by reference and are contained in 2 CFR § 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance). These Cooperative Agreement Financial & Administrative Terms and Conditions (CA-FATC) serve as the Foundation's implementation of 2 CFR § 200. **If the CA-FATC is silent on a specific area covered by 2 CFR § 200, requirements specified in 2 CFR § 200 must be followed**
- **5. Property Management Standards**. The awardee shall maintain a property management system that, at a minimum, meets the requirements of 2 CFR § 200.313(d). Because of increasing threats to information technology systems, the awardee is reminded that, under 2 CFR §§ 200.313(d)(3) and (4), "[a] control system must be developed to ensure adequate safeguards to prevent loss, damage, or theft of the property" and "[a]dequate maintenance procedures must be developed to keep the property in good condition." **This requirement imposes on the awardee a duty to adequately maintain and to insure adequate safeguards against the loss, damage, or theft of information technology equipment and systems purchased with NSF funds.**
- 31.c. All awards issued by NSF meet the definition of "Research and Development" (R&D) at 2 CFR § 200.87.



What Does NSF Tell You To Do? CA-FATC/LF, January 2016

- Cooperative Agreement Supplemental Financial & Administrative Terms and Conditions for Managers of Large Facilities,
- 60. Information Security
- Security for all information technology (IT) systems employed in the performance of this award, including equipment and information, is the **awardee's responsibility**. Within a time mutually agreed upon by the awardee and the cognizant NSF Program Officer, the awardee shall provide a written Summary of the policies, procedures, and practices employed by the awardee's organization as part of the **organization's IT security program, in place or planned, to protect research and education activities in support of the award**.
- The Summary shall describe the information security program appropriate for the project including, but not limited to: roles and responsibilities, risk assessment, **technical safeguards, administrative safeguards, physical safeguards**, policies and procedures, awareness and training, and notification procedures in the event of a cyber-security breach. The Summary shall include the institution's evaluation criteria that will measure the successful implementation of the IT Security Program. In addition, the Summary shall address appropriate security measures required of all subrecipients, researchers and others who will have access to the systems employed in support of this award.
- The Summary will be the basis of a dialogue which NSF will have with the awardee, directly or through **community meetings**. Discussions will address a number of topics, such as, but not limited to, evolving security concerns and concomitant cyber-security policy and procedures within the government and at awardees' institutions, available education and training activities in cyber-security, and **coordination activities among NSF awardees**.



Large Facility Manual Excerpts

June 2015

- *“Flexibility does not preclude rigor.”*
- Policies in Large Facilities Manual apply to all large facility projects funded by NSF, including:
 - Large facilities that have been or will be constructed or acquired with funds from the Major Research Equipment and Facility Construction (MREFC) Account;
 - Facilities or infrastructure projects that have been or will be constructed or acquired with funds provided through the Research and Related Activities (R&RA) and/or leveraged with Education and Human Resources (EHR) Accounts and that require National Science Board (NSB) approval; and
 - Existing facilities for which operation and replacement cost would be similar in size to MREFC-funded and MREFC-eligible projects.
- Program Officer has responsibility for: Monitors planning for IT and property security, and validates through periodic review
- Conceptual design phase – defining requirements, needs to include information security requirements
- **Commissioning Plan:** A listing of which cyber-security standards will be followed by the awardee and a description of how adherence to those standards will be verified. A policy for reporting to NSF of any breaches of cyber-security should also be given. This may be given as a reference to an existing cyber-security plan for the project.



More Large Facility Manual Excerpts

3.4 Project Execution Plan (PEP)

- **Section 12: Cyber-infrastructure:** includes the following specific components:
- **12.1 Cyber-Security Plan:** Plan for maintaining security of data, hardware, and networks during all stages of project life cycle.
- **12.2 Code Development Plan:** Plans for writing, testing and verifying, deploying, and documenting software, including configuration control during the stages of development.
- **12.3 Data Management Plan:** Plans for managing data, including infrastructure, archiving, open data access plans, etc. (cross-reference PAPPG)

3.5 Operations Plan

- All costs to operate, maintain and periodically upgrade the facility, its instrumentation and the IT components, including cost and approximate time of investment (Note: A PO can expect that IT components will need to be upgraded at least every 3 to 5 years);
- Are **SAFETY (emphasis added) (including IT security and security of the physical plant)**, environmental and health issues, if any, addressed?



Still More Large Facility Manual Excerpts

4.2.2 Cost Estimating and Analysis for Construction Awards

- **All cyber-infrastructure costs** (both initial cost and **continuing costs** of hardware, software, maintenance, upgrades and operations) are fully considered. **Rapid advances in computing may require upgrades as often as every 3 to 5 years.**

4.2.3 Cost Estimating and Analysis for Operations Awards

- Salary costs categories typically include: professionals and technicians to operate and maintain the facility; **IT and cyber-infrastructure specialists**; administrative and grounds staff; environmental, health and safety specialists; machinists; designers, engineers and software experts to support users; engineers/scientists to conduct research and development (R&D) for continuous improvement to the facility and related instrumentation; liaison staff to interface with the community; project management specialists for ongoing projects; financial and budget specialists; and staff to meet reporting requirements
- Other examples of **items that may require separate consideration** are expendables – such as cryogenes, gases and spare parts – and ancillary equipment such as refrigerators and **IT equipment**. Planners should **assess emerging IT and cyber-infrastructure technologies, such as grid computing**, to ensure that the research community will have appropriate resources to make best use of the data and to assume leadership roles in the field. **Initial IT capital costs and the cost of software development, including software support during operations, need to be carefully evaluated.** Furthermore, informed estimates regarding the small- and mid-scale instrumentation needs of the facility and users of the facility should be made.
- **While specific computing costs generally drop with time (Moore's Law), the data volume is increasing at least as fast, and greater and greater bandwidth is required for the transmission of data to remote users. As a result, the time frame for IT upgrades/turnover is typically three to four years.**



Finally, the Last Large Facility Manual Excerpts

- 5.2 Risk Management Guidelines
- 5.3 Guidelines for cyber-security of NSF's Large Facilities
 - NSF has responsibility for oversight of facilities it constructs and operates, including associated IT Infrastructure.
 - This section, to be written, will describe what NSF considers to be a fundamental set of IT security requirements that facilities should consider in developing and deploying their IT plans, policies and procedures.
 - These minimal requirements and their associated evaluation criteria, as provided by the facility and agreed to by NSF, are used as part of NSF's facility oversight and review process.
 - This module will document NSF's expectation for the recipient and PO oversight for the implementation and monitoring of cyber-security best practices.
 - These expectations extend over the full life cycle of an award, and are appropriately modified as the award passes through various stages of its life cycle.
- The LFM is our opportunity to shape our future... *"Compliance is Imminent..."*

USAP Information Security Policies



United States Antarctic Program

[Home](#)[Contact Us](#)[Station Times](#)[Quick Links](#)[Advanced Search](#)

Information Security Policies and Instructions

[Home](#) | [IT Comms](#) | [Information Security](#)

United States Antarctic Program (USAP) information security policies and instructions address federal requirements for information security standards on government networks. All USAP participants with access to the USAP network should be familiar with the policies and instructions.



FUTURE USAP
The latest information on the USAP master plans and their implementation.

[About the USAP](#)[About Antarctica](#)[Grantee Support](#)[Program Operations](#)[Calendars and Schedules](#)[Conferences, Committees, and Workshops](#)[Logistics](#)[Vessel Science and Operations](#)

| Policy Number | Policy Title |
|----------------------|---|
| EntROB | USAP Enterprise Information Infrastructure (Enterprise Rules of Behavior) ▲ |
| Acknowledgement Form | Acknowledgement of Information Security Policies ▲ |
| SenROB | Sensitive Rules of Behavior and Acknowledgement ▲ |
| 5000.01 | The USAP Information Security Program ▲ |
| 5000.02 | Information Security Organization and Administration ▲ |
| 5000.03 | Information Categorization ▲ |
| 5000.04 | Risk Management ▲ |
| 5000.05 | Information Security Architecture ▲ |
| 5000.06 | Acceptable Use of USAP Information Resources ▲ |

Another Quiz...

Risk Management Planning

1. Risk Identification
2. Qualitative Risk Analysis
3. Quantitative Risk Analysis
4. Risk Response Planning
5. Risk Monitoring and Control

Shackleton's Hut at Cape Royds, Ross Island, 1907
Shackleton had to abandon his trek to Pole...

...not enough food for the return trip



Risk Management Process – The LFO Way

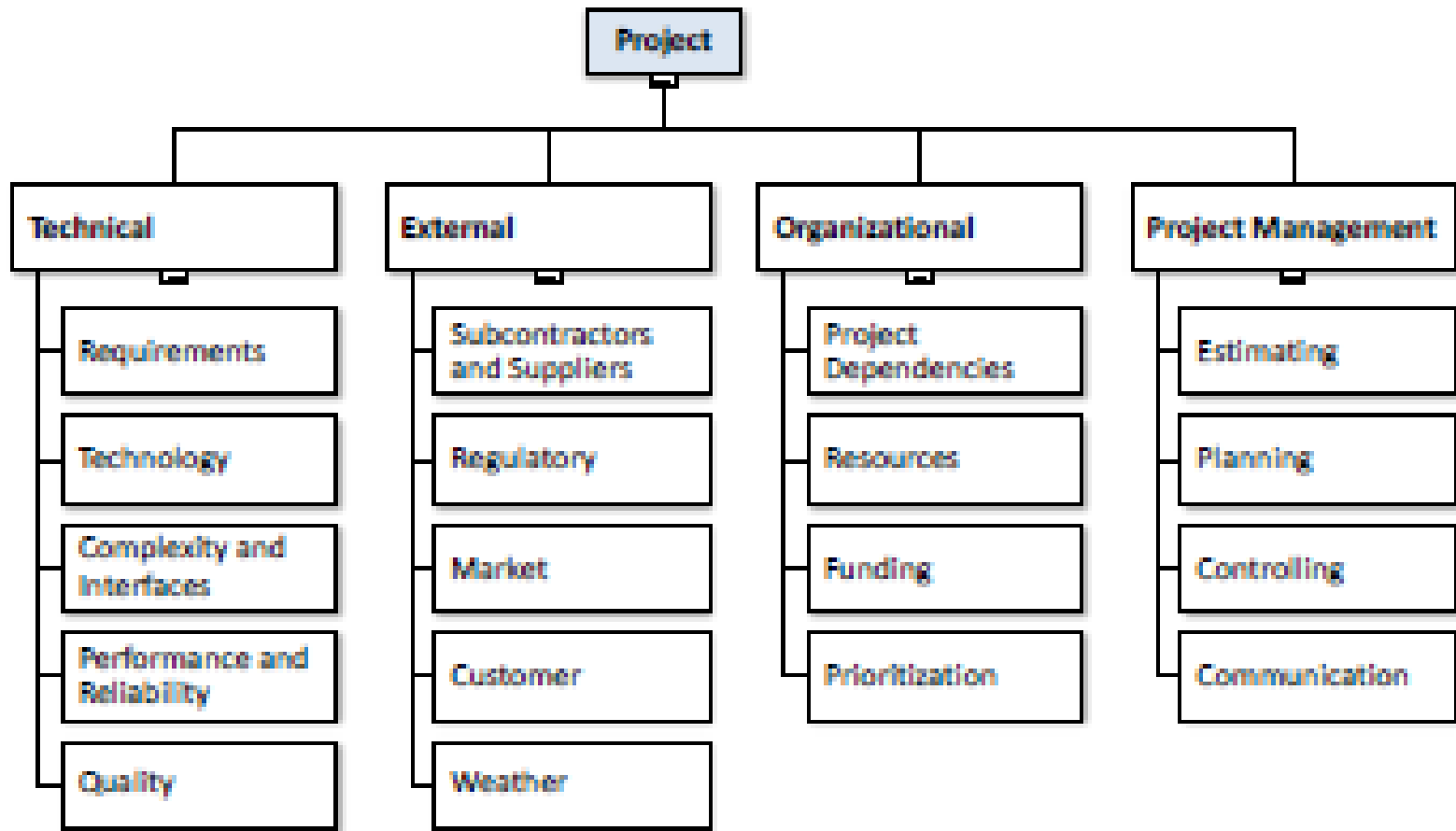
Figure 5.2.4-1 Picture of Six Risk Management Processes (According to PMI)³





LF Manual: Typical Risk Breakdown Structure

Figure 5.2.6-2 Typical Risk Breakdown Structure (RBS)¹





Another Approach: OMB Risk Categories

Figure 5.2.6-3 OMB Risk Categories: to be used as a starting point for projects to select their own categories

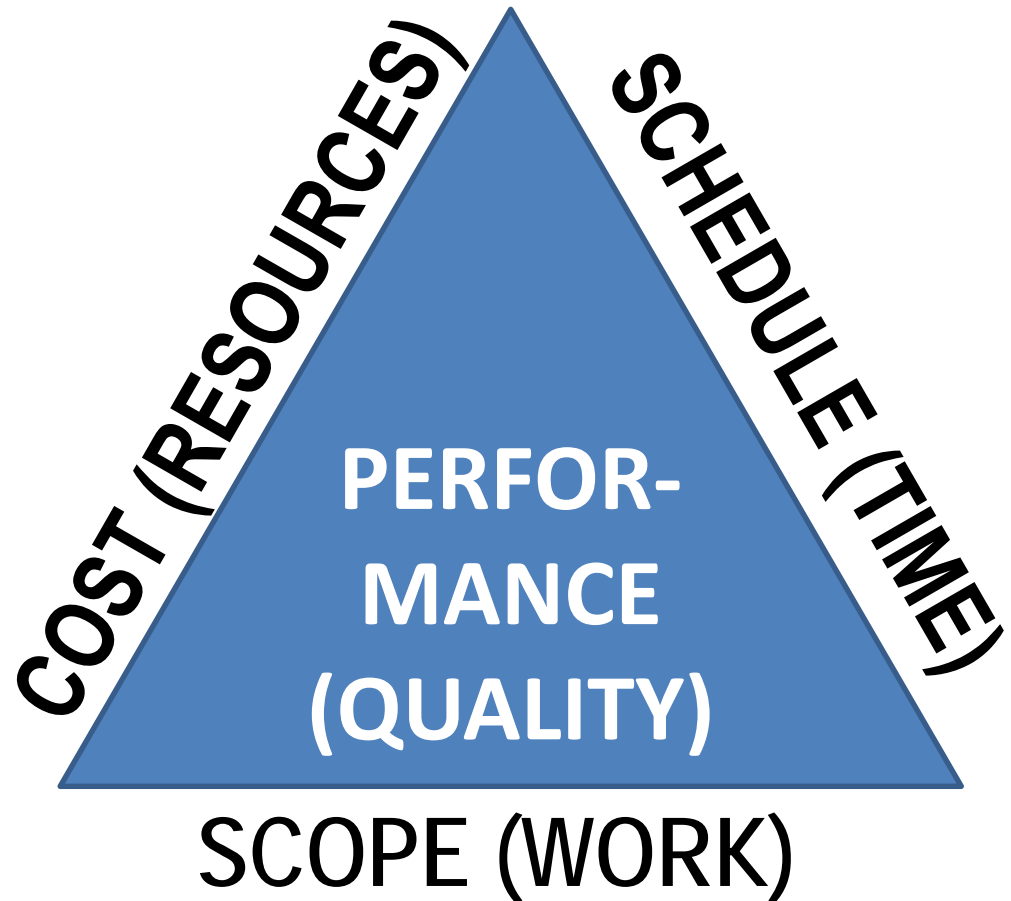
- | | |
|---|--|
| 1) Schedule | 11) Overall Risk of Project Failure |
| 2) Initial Costs | 12) Organizational and Change Management |
| 3) Life Cycle Costs | 13) Business |
| 4) Technical Obsolescence | 14) Data/Info |
| 5) Feasibility | 15) Technology |
| 6) Reliability of Systems | 16) Strategic |
| 7) Dependencies and Interoperability | 17) Security |
| 8) Surety (Asset Protection) | 18) Privacy |
| 9) Risk of Creating a Monopoly | 19) Project Resources |
| 10) Capability of Agency to Manage the Investment | |

- **Technical Obsolescence**
- **Data/Info**
- **Technology**
- **Security**



Project Management Body Of Knowledge (PMBOK)

- The Large Facilities Manual is a basic resource.
- Project Management 101: Scope (Work), Schedule (Time), Cost (Resources), Performance (Quality);
- Cybersecurity is a Program
 - Series of interrelated projects
- Project management concepts also apply to Operations Management
- Definite start and Definite ends exist within the concept of “ongoing operations,” e.g. Shift work; maintenance windows to avoid primary science time



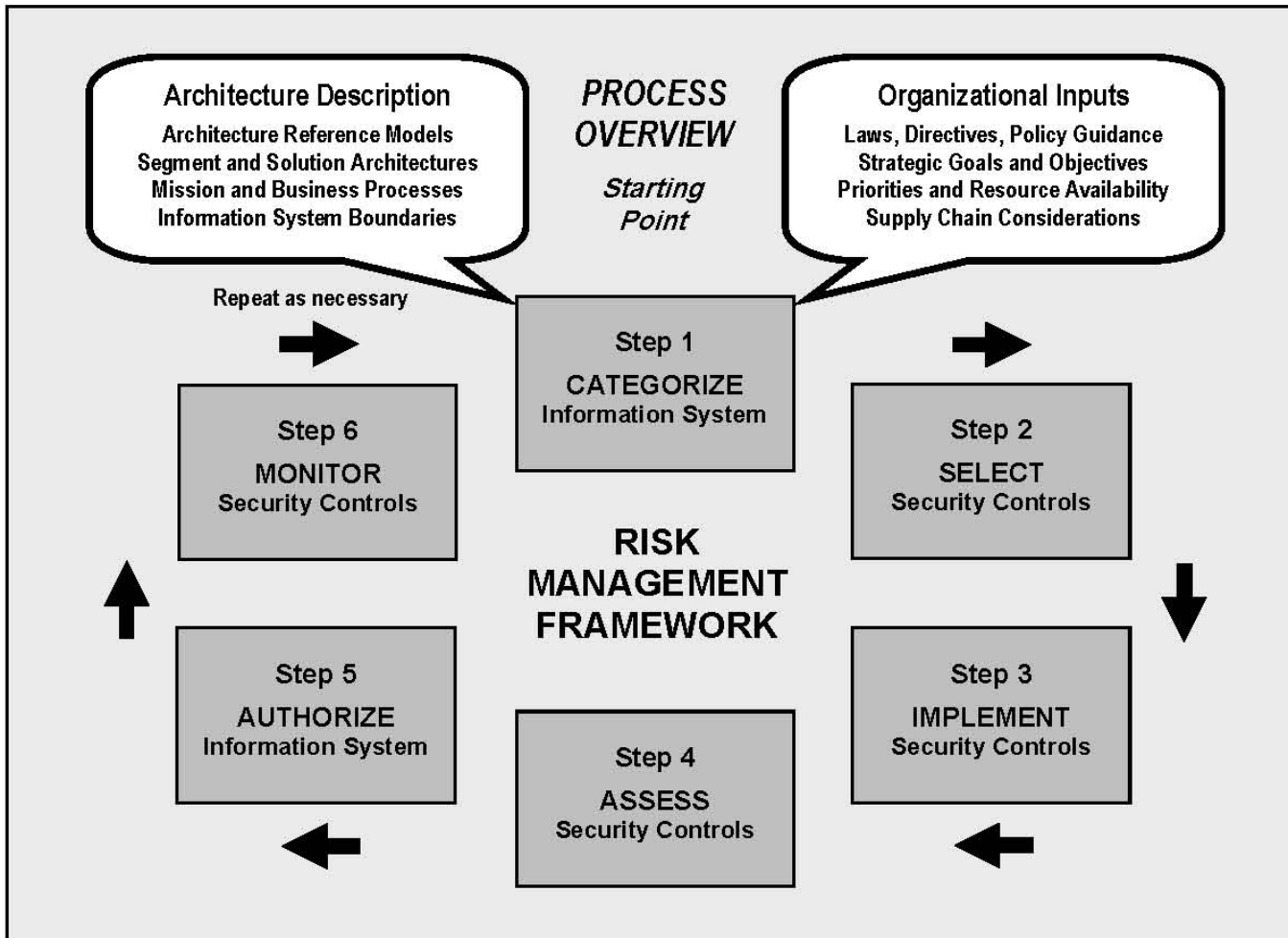


NIST and the Risk Management Framework

- FISMA assigns to NIST the responsibility for developing standards and guidelines for federal agencies to use for implementing information/cybersecurity
- OMB directs agencies to use NIST Risk Management Framework and NIST controls catalog (Circular A-130, July 2016, other OMB memos)
- **NIST Special Publication (SP) 800-39, *Managing Information Security Risk; Organization, Mission, and Information System View*;**
- **SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*;**
- **FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*;**
- **SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*;**
- **FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*;**
- **SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*;**
- **“This publication may be used by nongovernmental organizations on a voluntary basis”**



Hmm, this looks familiar...





Risk Management Approaches Compared

| Step | Activity | LFO Risk Management |
|---|--|--|
| 1. Categorize Information Systems | <ul style="list-style-type: none"> ▪ Review using FIPS 199 & SP 800-60 | 1. Risk Identification |
| 2: Select Security Controls | <ul style="list-style-type: none"> ▪ Apply identified baseline controls; ▪ Tailor controls based on operational needs, technology constraints, budget; ▪ Document controls in System Security Plan; presented by System Owner; approved by Authorizing Official (AO). | 1. Risk Identification 2. Qualitative Risk Analysis 3. Quantitative Risk Analysis |
| 3: Implement Security Controls | <ul style="list-style-type: none"> ▪ Use people, process, technology to implement controls | 4. Risk Response Planning |
| 4: Assess Security Controls | <ul style="list-style-type: none"> ▪ Annually review subset of controls; independent assessor required for Moderate & High. | 2. Qualitative Risk Analysis 3. Quantitative Risk Analysis 4. Risk Response Planning |
| 5: Authorize Information Systems | <ul style="list-style-type: none"> ▪ AO issues Authorization To Operate (ATO) if the risk of operating the system is considered acceptable based on mission considerations and evaluation of alternatives to not operating | 2. Qualitative Risk Analysis 3. Quantitative Risk Analysis 4. Risk Response Planning |
| 6: Continuously Monitor Security Controls | <ul style="list-style-type: none"> ▪ AO ensures continuously monitors controls to maintain current assessment of risk and to identify opportunities to reduce risk. ▪ Funding is key to success. | 5. Risk Monitoring and Control |

USAP Information Security Risk Management

- What Risks do we accept by the choices we make:
 - What could go wrong? (the IT Loss);
 - What are we doing to reduce the Risk? (the IT Response);
- InfoSec Risk has 3 basic objectives: Protect Confidentiality, Integrity, Availability;
 - Confidentiality Loss: unauthorized access to or use of our systems/network, or to our sensitive data, e.g. illegal downloading of copyrighted material;
 - Integrity Loss: unauthorized modification of our data, e.g. amount of fuel available for winter operations;
 - Availability Loss: unauthorized/unplanned disruption of our IT services, e.g. satellite communications outage affects station off-continent communications;
- Probability/Likelihood of Loss Occurrence:
 - We are a .gov network: we are a target;
 - We have older IT infrastructure: we will have outages;
- The Response: What are we doing?
- We organize Program Operations to reduce the Impact of IT Loss:
 - Life Safety impacts of IT loss are mitigated by on-station medical services and redundant communications capabilities, e.g. High Frequency Radio and Iridium satellite telephones;
 - Science impacts of IT loss are mitigated by grant team activities, e.g. data backups, Iridium field party communications;
- Part of overall Enterprise Risk Management Approach: Risk Consideration governs everything we do in Antarctica



USAP Information Security Program

- Infosec Risk Management Program built around statutory requirements (FISMA), mandatory standards (NIST) and annual implementation guidance (OMB);
- NIST Risk Management Framework:
 - Identify risks and respond with controls, commensurate with magnitude of harm that could result from loss (NIST, OMB);
 - Assess controls annually; continuous monitoring for some controls through Continuous Diagnostics and Mitigation (CDM) initiative (NIST, OMB);
 - OIG Independent Evaluation (FISMA);
- Continually evaluate IT investment to balance security investments against operational investments; we need to do science, securely;
- Current Info/CyberSec investments of ~\$3M (Primarily Labor) (ASC and SPAWAR)
- Represents ~12.5% of overall USAP IT spend (~\$24M);
- Represents 1.1% of overall USAP Logistics & Infrastructure budget (\$262.63M)
- Consistent with Small/Medium Business (SMB) spending per PWC 2015 survey

South Pole MedEvac, June 2016:
What are the Risks?
What is the FIPS 199 Probable Impact?





The RMF and IceCube – A Notional Review

- **What if IceCube was a Federal information system, how would it stack up against the RMF?**
- Step 1: Categorize IceCube using FIPS 199 and SP 800-60 (about 1 hour (SME)).
- FIPS 199: The security categories are based on the **potential impact** on an organization should certain events occur which jeopardize the information and information systems needed by the organization to
 - Accomplish its assigned mission,
 - Protect its assets,
 - Fulfill its legal responsibilities,
 - Maintain its day-to-day functions, and
 - Protect individuals.
- What is the potential impact on IceCube? The University of Wisconsin and the other Partners? The NSF?
- SP 800-60: What types of Information are contained within IceCube?



FIPS 199 Potential Impact Levels

- **LOW: Limited** Adverse Effect on operations, assets, or individuals:
 - (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
 - (ii) result in minor damage to organizational assets;
 - (iii) result in minor financial loss; or
 - (iv) result in minor harm to individuals.
- **MODERATE: Serious** Adverse Effect on operations, assets, or individuals:
 - (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
 - (ii) result in significant damage to organizational assets;
 - (iii) result in significant financial loss; or
 - (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
- **HIGH: Severe or Catastrophic** Adverse Effect on operations, assets, or individuals:
 - (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
 - (ii) result in major damage to organizational assets;
 - (iii) result in major financial loss; or
 - (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
- ***Application of definitions must take place within context of organization and overall national interest.***



Summary Notional Information Categorization for IceCube

| Information Type | C | I | A |
|--|-----|-----|-----|
| C.2.4.1 Contingency Planning Information Type | MOD | MOD | MOD |
| C.3.5 Information and Technology Management | | | |
| C.3.5.1 System Development Information Type | LOW | MOD | LOW |
| C.3.5.2 Lifecycle/Change Management Information Type | LOW | MOD | LOW |
| C.3.5.3 System Maintenance Information Type | LOW | MOD | LOW |
| C.3.5.4 IT Infrastructure Maintenance Information Type | LOW | LOW | LOW |
| C.3.5.5 Information Security Information Type | LOW | MOD | LOW |
| C.3.5.7 Information Management Information Type | LOW | MOD | LOW |
| C.3.5.8 System and Network Monitoring Information Type | MOD | MOD | LOW |
| D.19.1 Scientific and Technological Research and Innovation Information Type | LOW | MOD | LOW |
| D.19.2 Space Exploration and Innovation Information Type | LOW | MOD | LOW |
| D.20.1 Research and Development Information Type | LOW | MOD | LOW |

Security Category = {(confidentiality, MODERATE), (integrity, MODERATE), (availability, MODERATE)} (unless we can define reasons for it being LOW)

This is the value of tailoring following a consistent approach: Each impact rating can be adjusted based on the organization's mission.



Risk Management Framework & IceCube – Summary

| Step | Activity | IceCube |
|---|--|--|
| 1: Categorize Information Systems | <ul style="list-style-type: none"> Review using FIPS 199 & SP 800-60 | <ul style="list-style-type: none"> Notional Categorization Moderate (800-60) |
| 2: Select Security Controls | <ul style="list-style-type: none"> Apply identified baseline controls; Tailor controls based on operational needs, technology constraints, budget; Document controls in System Security Plan; presented by System Owner; approved by Authorizing Official (AO). | <ul style="list-style-type: none"> Need to tailor baseline (CTSC Leadership Opportunity) SSP submitted to NSF as part of new CA award (2016) (CA-FATC) |
| 3: Implement Security Controls | <ul style="list-style-type: none"> Use people, process, technology to implement controls | <ul style="list-style-type: none"> Ongoing |
| 4: Assess Security Controls | <ul style="list-style-type: none"> Annually review subset of controls; independent assessor required for Moderate & High. | <ul style="list-style-type: none"> Ongoing, e.g. CTSC Engagement |
| 5: Authorize Information Systems | <ul style="list-style-type: none"> AO issues Authorization To Operate (ATO) if the risk of operating the system is considered acceptable based on mission considerations and evaluation of alternatives to not operating | <ul style="list-style-type: none"> Need to check status; is there an equivalent activity? Who at the institution? |
| 6: Continuously Monitor Security Controls | <ul style="list-style-type: none"> AO ensures continuously monitors controls to maintain current assessment of risk and to identify opportunities to reduce risk. Funding is key to success. | <ul style="list-style-type: none"> Ongoing |

Services

Office 365, Google Apps, software, more

Learn

Helpful IT guides and training

IT Community

IT governance, groups and resources

About

Learn about IT at UW-Madison

 Search the UW IT site

[Home](#) > [About](#) > [Office of the CIO](#) > [IT policies](#)

IT policies

[Top policies](#)

[All policies](#)

[Related documents](#)

[Last reviewed](#)

- [Access Control Services Policy](#)
- [Access Control Services Standard](#)
- [Access to Faculty and Staff Electronic Files Policy](#)
- [Cellular Phones Policy](#)
- [Collection of PII via Email Policy](#)
- [Data Classification Policy](#)
- [Disposal and Reuse Policy](#)
- [Disposal and Reuse Procedures](#)
- [Electronic Devices Policy](#)
- [Email Servers Policy](#)
- [Guest NetID Policy](#)
- [Incident Reporting and Response Policy](#)
- [Incident Reporting and Response Procedures](#)
- [IPv4 Allocation Policy](#)
- [NetID Eligibility Policy](#)
- [Password Policy](#)
- [Password Standard](#)
- [Responsible Use Policy](#)
- [Restricted Data Management Policy](#)
- [Restricted Data Management Procedures](#)
- [Sensitive Information Definition](#)
- [Storage and Encryption Policy and Standard](#)
- [Storage and Encryption Standard](#)
- [Telephone Usage Policy](#)
- [UDS Responsible Use Policy](#)
- [Vulnerability Scanning Policy](#)
- [Web Accessibility Policy](#)
- [Web Accessibility Procedures](#)

[IT Policy Knowledgebase](#)

[Contact us](#)

IT Policy Forum

April 27, 2016

Topic

Presentation and discussion of the recommendations of the Non-UW-Madison Devices and Services Team (a.k.a. BYOD and Cloud Services)

Introduction by [Bruce Maas](#), CIO and Vice Provost for Information Technology

University of Wisconsin IT Policies



Ideas on the Risk Management Framework & Science CyberInfrastructure

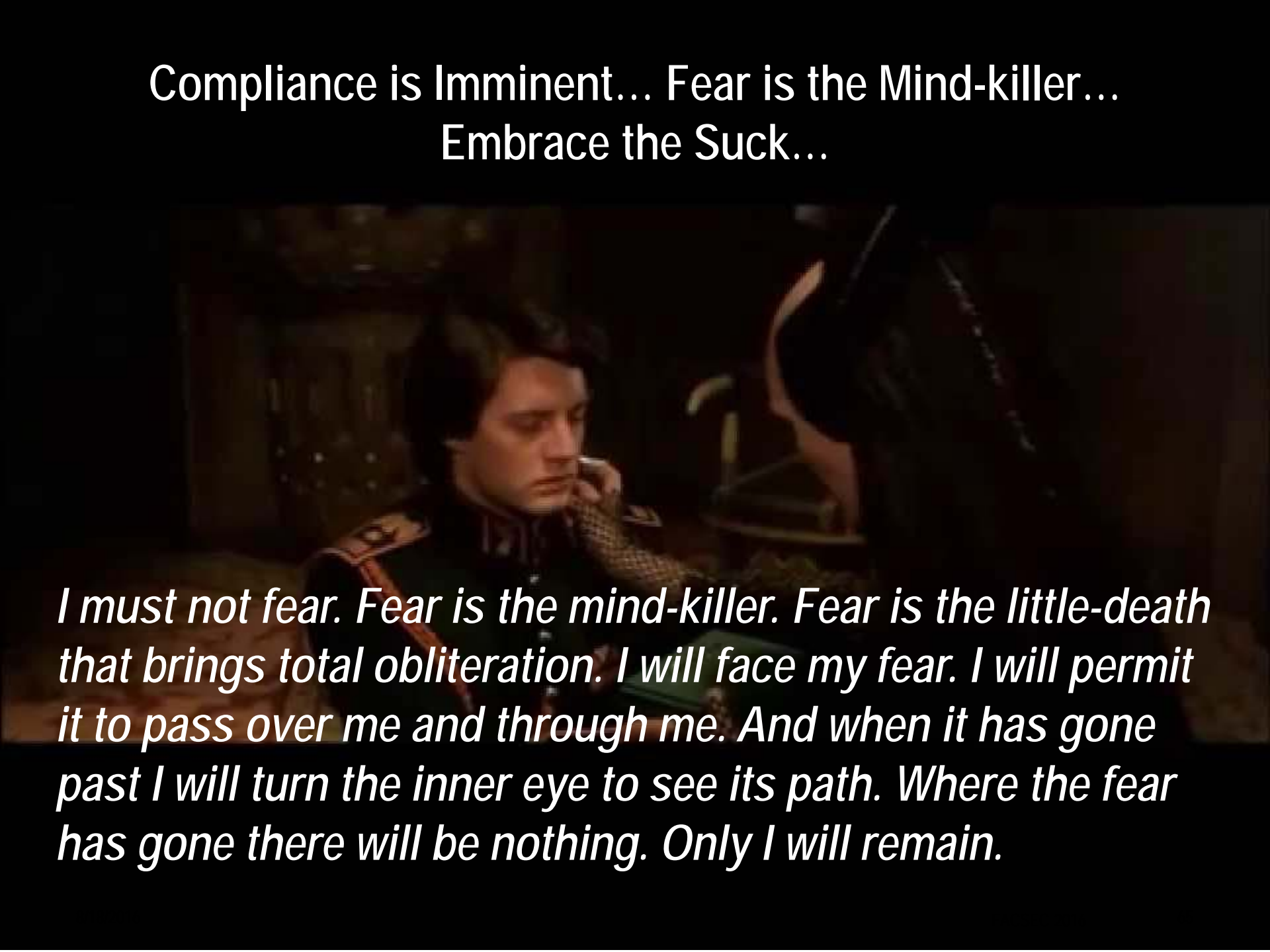
- Go Big or Go Home
 - Large Facilities are Large Investments – size, commitment of resources, commitment of time to develop, build and operate;
 - We need to apply Project Management concepts to all aspects of our Information Security Programs.
- Like the facilities themselves, cyberinfrastructure investments will remain with us for many years, we are building the legacy systems that we will be operating in 10 years
 - IceCube Lab was originally an elevated dormitory built in 1994
 - South Pole primary off-station communications relies on satellites that are past their designed service life, as much as 20 years as more.
- In some cases, we will intentionally repurpose information systems that were not intended to support our operations.
 - GOES-3, DSCS, Iridium
- The future of science remains collaboration, especially for the large facilities we operate today.
- What's an ISM to do?



Ideas on the Risk Management Framework

- The Fourth Option: We are already doing the Risk Management Framework, might as well claim credit for it.
- If we as the cybersecurity expertise for cyberinfrastructure evaluate the NIST Risk Management Framework more thoroughly, we can define standard approaches for adapting the RMF to unique science mission programs.
- At the same time, we can become a resource for smaller grant teams, smaller institutions, and small agencies.
- “Federal information” and “by or on behalf of”
- Updates to PAPPG, CA-FATC, CA-FATC/LF, LF Manual to include information security requirements.

Compliance is Imminent... Fear is the Mind-killer...
Embrace the Suck...

A man with dark hair, wearing a dark uniform with a patterned shoulder strap, is seated at a desk. He is looking down and to the right with a serious, contemplative expression. The background is dark and indistinct.

I must not fear. Fear is the mind-killer. Fear is the little-death that brings total obliteration. I will face my fear. I will permit it to pass over me and through me. And when it has gone past I will turn the inner eye to see its path. Where the fear has gone there will be nothing. Only I will remain.



BACKGROUND SLIDES



Notional Information Categorization for IceCube

| Information Type | Description | C | I | A |
|--|---|-----|-----|-----|
| C.2.4.1 Contingency Planning Information Type | <ul style="list-style-type: none"> • Actions required to plan for, respond to, and mitigate damaging events. | MOD | MOD | MOD |
| C.3.5 Information and Technology Management | <ul style="list-style-type: none"> • Coordination of IT resources and systems required to support or enable a citizen service. • Impacts to information associated with the operation of IT systems generally need to be considered even when all mission-related information processed by the system is intended to be available to the general public. • The relevant issues may be different for integrity and availability than for confidentiality. • Information that has been made public, by definition, requires no confidentiality protection. • In contrast, integrity and availability protection cannot be maintained for copies of information that have been distributed to the public. • Integrity and availability assurance can only be maintained by maintaining copies of information in organization-controlled information systems. | | | |
| C.3.5.1 System Development Information Type | <ul style="list-style-type: none"> • All activities associated with the in-house design and development of software applications. | LOW | MOD | LOW |
| C.3.5.2 Lifecycle/Change Management Information Type | <ul style="list-style-type: none"> • Processes that facilitate a smooth evolution, composition, and workforce transition of the design and implementation of changes to agency resources such as assets, methodologies, systems, or procedures. | LOW | MOD | LOW |
| C.3.5.3 System Maintenance Information Type | <ul style="list-style-type: none"> • All activities associated with the maintenance of in-house designed software applications. | LOW | MOD | LOW |



Notional Information Categorization for IceCube

| Information Type | Description | C | I | A |
|--|--|-----|-----|-----|
| C.3.5.4 IT Infrastructure Maintenance Information Type | <ul style="list-style-type: none"> Involves the planning, design, implementation, and maintenance of an IT Infrastructure to effectively support automated needs (i.e. operating systems, applications software, platforms, networks, servers, printers, etc.). IT infrastructure maintenance also includes information systems configuration and security policy enforcement information. This information includes password files, network access rules and implementing files and/or switch setting, hardware and software configuration settings, and documentation that may affect access to the information system's data, programs, and/or processes. The impact levels associated with IT infrastructure maintenance information are primarily a function of the information processed in and through that infrastructure. The IT Maintenance Information type represents a complex set of data elements that are used to secure the design, implementation, and maintenance of systems and networks. The security of each of these data elements is dependent on the security of the other data elements. Security compromise of one data element type will propagate to others. | LOW | LOW | LOW |
| C.3.5.5 Information Security Information Type | <ul style="list-style-type: none"> All functions pertaining to the securing of Federal data and systems through the creation and definition of security policies, procedures and controls covering such services as identification, authentication, and non-repudiation. | LOW | MOD | LOW |
| C.3.5.7 Information Management Information Type | <ul style="list-style-type: none"> Coordination of information collection, storage, and dissemination, and destruction Managing the policies, guidelines, and standards regarding information management. | LOW | MOD | LOW |
| C.3.5.8 System and Network Monitoring Information Type | <ul style="list-style-type: none"> All activities related to the real-time monitoring of systems and networks for optimal performance. System and network monitoring describes the use of tools and observation to determine the performance and status of information systems and is closely tied to other Information and Technology Management sub-functions. System and network monitoring information type should be considered broadly to include an agency's network [performance, health, and status] and security operations [intrusion monitoring, auditing, etc.] support. | MOD | MOD | LOW |



Notional Information Categorization for IceCube

| Information Type | Description | C | I | A |
|--|---|-------------|-----|-----|
| D.19.1 Scientific and Technological Research and Innovation Information Type | <ul style="list-style-type: none"> All federal activities whose goal is the creation of new scientific and/or technological knowledge as a goal in itself, without a specific link to the other mission areas or information types identified in the BRM. Most sensitive information is developed under research and development programs that directly support another of the mission areas described in this Appendix and are not included here. | LOW | MOD | LOW |
| D.19.2 Space Exploration and Innovation Information Type | <ul style="list-style-type: none"> All activities devoted to innovations directed at human and robotic space flight Development and operation of space launch and transportation systems, and the General research and exploration of outer space. Most sensitive information is developed under research and development programs that directly support another of the mission areas described in this Appendix and are not included here. | LOW/ MOD | MOD | LOW |
| D.20.1 Research and Development Information Type | <ul style="list-style-type: none"> Gathering and analysis of data, Dissemination of results, and Development of new products, methodologies, and ideas. Sensitivity and criticality of most research and development information depends on the subject matter involved. | LOW | MOD | LOW |