National Science Foundation

Division of Polar Programs

Arctic Sciences Section

Information Security Handbook

Version 2.2

Distribution: All Arctic Sciences Section (ARC) Employees, Contractors, Subcontractors, Cooperative Agreements, Grant Agreements, and Participants

Cancellation Date: Effective Until Cancelled

Originating Unit: National Science Foundation, Division of Polar Programs, Arctic Sciences Section

Originating Year: 2012

NSF PLR ARC Information Security Handbook Revisions

Version	Date	Section	Description	Changes by
V 0.1	6/28/2012	Throughout	Initial draft	ARC Information Security Team
V 0.2	9/12/2012	Throughout	Information Assurance Working Group (IAWG) feedback revision	ARC Information Security Team
V 0.3	10/10/2012	Throughout	ARC RSL Program Manager feedback revision	ARC Information Security Team
V 1.0	10/12/2012	Throughout	Final	ARC Information Security Team
V 1.1	4/17/2013	Throughout	Changed references to Office of Polar Programs (OPP) to Division of Polar Programs	ARC Information Security Team
V1.2	6/4/2013	Chapter IV	Addition of Chapter IV. Privacy Policies.	ARC Information Security Team
V1.3	10/31/2013	Throughout	Verified references to Arctic Sciences Section (ARC).	ARC Information Security Team
V1.4	3/15/2014	Chapter III & References	Personnel Security Requirements & References	ARC Information Security Team
V1.5	5/5/2014	Chapter III Incident Response , Chapter IV Privacy Policies, Appendix C	Updated Incident Response, Privacy References, Added Appendix C	ARC Information Security Team
V1.6	5/27/2014	Figure 1	Update to ARC Authorization Boundary diagram	ARC Information Security Team
V1.7	4/21/2015		Added Incident Response Plan and Risk Management Plan	ARC Information Security Team
V1.8	4/29/2015	Chapter II, Chapter III, Appendices C & D	Added Hardware and Software Maintenance Policy, Updated Incident Response and Risk Assessment sections and appendices	

V1.9	5/1/2015	Chapter II	Updates to Risk Assessment section	ARC Information Security Team
V 2.0	5/28/2015	Throughout	Included comments from ALEX review	ARC Information Security Review
V 2.1	6/10/15	Throughout	Included changes requested by RSL PMs	ARC Information Security Team
V 2.2	9/28/2015	Throughout	Included changes requested by RSL PMs	ARC Information Security Team

Executive Summary

This handbook provides the framework for National Science Foundation (NSF) Division of Polar Programs (PLR) Arctic Sciences Section (ARC) implementation and maintenance of the ARC Information Security Program in accordance with the Federal Information Security Management Act (FISMA).

The intent of this handbook is to provide policies to all ARC Program Participants and service providers, to address Federal information security requirements consistent with National Institute of Standards and Technology (NIST) and Office of Management and Budget (OMB) guidelines, and industry best practices.

This handbook is structured as follows:

- *Chapter I*: Overview of ARC Information Security Program and synopsis of the Arctic RSL Program purpose.
- *Chapter II*: Management control policies which focus on administration of IT and the management of risk for systems supporting the ARC Program.
- *Chapter III*: Operational control policies which address security methods focusing on mechanisms implemented and executed by people, as opposed to systems.
- *Appendix A*: Glossary of definitions and terms used throughout this handbook.
- *Appendix B*: References
- *Appendix C*: Arctic Incident Response Plan
- *Appendix D*: ARC VRAT Management Process

The material in this handbook promulgates specific policies and procedures to protect confidentiality, integrity, and availability of ARC Program data and IT systems. All systems require some level of protection, which is determined by evaluating the sensitivity and criticality of the information processed, the relationship of the system to the organization's mission, and the economic value of the system's components.

This handbook describes the requirements under FISMA and OMB Circular A-130, *Management of Federal Information Resources*, to:

- Ensure integrity, confidentiality, authenticity, availability, and non-repudiation of information and information systems supporting ARC operations and assets.
- Develop and implement information security policies, procedures, and control techniques.

This handbook is reviewed in conjunction with major changes to ARC Program information infrastructure, or no less than annually.

Audience

The ARC Information Security Handbook is intended for reference and use by service providers, researchers, and benefactors of the ARC Program. The Information Security boundary as defined in this handbook and the program System Security Plans are limited to those assets managed by contractors. Information security for IT assets provided by grantees or cooperative agreement is outside the scope of this handbook, however guidance may sometimes be included as a best practice. The audience for this document includes the following entities:

- *Agency* –NSF ARC Research Support and Logistics (RSL) Program Management responsible for ARC adherence to Federal information security regulations.

- *Contractor* - Commercial organizations (contractors/subcontractors) providing property or services to ARC.
- *Cooperative Agreement (CA)* – Educational institutions, state, or local governments in providing support authorized by ARC via a Cooperative Agreement.
- *Grant Agreement (GA)* – Support or research issued by ARC provided under a GA to accomplish a public purpose of support.

Policies throughout this document may be labeled with *Federal*, *CO*, *CA* and/or *GA* to identify specific requirements that apply to each of these audiences. While those providing services under CA are only *required* to comply with the procedures of their own institution, they should review and be familiar with the guidance in this handbook as it is required of contractors who may be working at the facilities operated by the CA. Individual policy statements may also reference the *end user* who are individuals belonging to one of the primary audiences listed above. In cases where the *end user* is referenced, the individual and the affiliated organization are responsible for ensuring compliance with the policy requirement.

Compliance

Failure to comply with policies presented in this handbook shall result in escalation to ARC RSL Program Managers for resolution. Consequences for non-compliance are at the discretion of ARC RSL Program Managers.

Acronyms

Acronyms used throughout this handbook are defined below.

Table 1. Acronyms

Acronym	Definition
ARC	Arctic Sciences Section
CPO	Chief Privacy Officer
CP	Contingency Planning
CO	Contract
CA	Cooperative Agreement
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
GSS	General Support System
GA	Grant Agreement
IR	Incident Response
MP	Media Protection
NIST	National Institute of Standards and Technology
NSF	National Science Foundation
OIG	Office of Inspector General

Acronym	Definition
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIRT	PII Incident Response Team
PLR	Division of Polar Programs
POA&M	Plan of Action and Milestones
RSL	Research Support and Logistics
RA	Risk Assessment
RMF	Risk Management Framework
SA&A	Security Assessment and Authorization
SP	Special Publication
SSP	System Security Plan
SCA	Security Control Assessment
SI	Sensitive Information
VM	Vulnerability Management

Chapter I. ARC Information Security Program Overview

The ARC Information Security Program is established in accordance with requirements of FISMA, OMB Circular A-130, and related Federal information security guidance. This document applies to the information technology provided through the Arctic Research Support and Logistics Program, in particular those supported through the Arctic Research Support and Logistics Services contract and the Alternative Experts contracts. Compliance with this policy is as indicated in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4.

Security Support for the Arctic Research Support and Logistics Program

The ARC Information Security Program is designed to ensure adequate security measures are in place to address security considerations directly related to ARC Program mission and supporting business processes. Aligning implementation of security policies with the Arctic RSL Program mission ensures that information security is consistent with an organizational risk management strategy. As stated in the Arctic RSL Program Synopsis available on the NSF website[1]:

> *The Arctic Research Support and Logistics (RSL) Program supports the fieldwork of research projects funded through science programs in the Arctic Sciences Section … and in some cases proposals funded elsewhere at NSF and at other agencies. The RSL program also supports facilities and services to the research community through grants, cooperative agreements and contracts to organizations. The RSL program invests in some research and development activities to improve efficiency, safety and access to the Arctic.*

The primary focus of the ARC Information Security Program is to ensure confidentiality, integrity, and availability of Personally Identifiable Information (PII) and Sensitive Information (SI) managed by and on behalf of the ARC Program. The ARC Information Security Program is also focused on ensuring the security of systems essential for the operation of Arctic sites. For more information on systems supporting the ARC Program please refer to the System Security Plan (SSP).

Authorization Boundaries

ARC authorization boundaries are based on the definitions provided by OMB Circular A-130, Appendix III:

- *General Support System* – An interconnected set of information resources under the same direct management control that shares common functionality. A GSS typically includes hardware, software, information, data, applications, communications, and people. Direct management control is budgetary and operational authority for the day-to-day maintenance of the information systems.
- *Key Application* – An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

ARC authorization boundaries are depicted in Figure 1.

[1] http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=13437&org=ARC&from=home

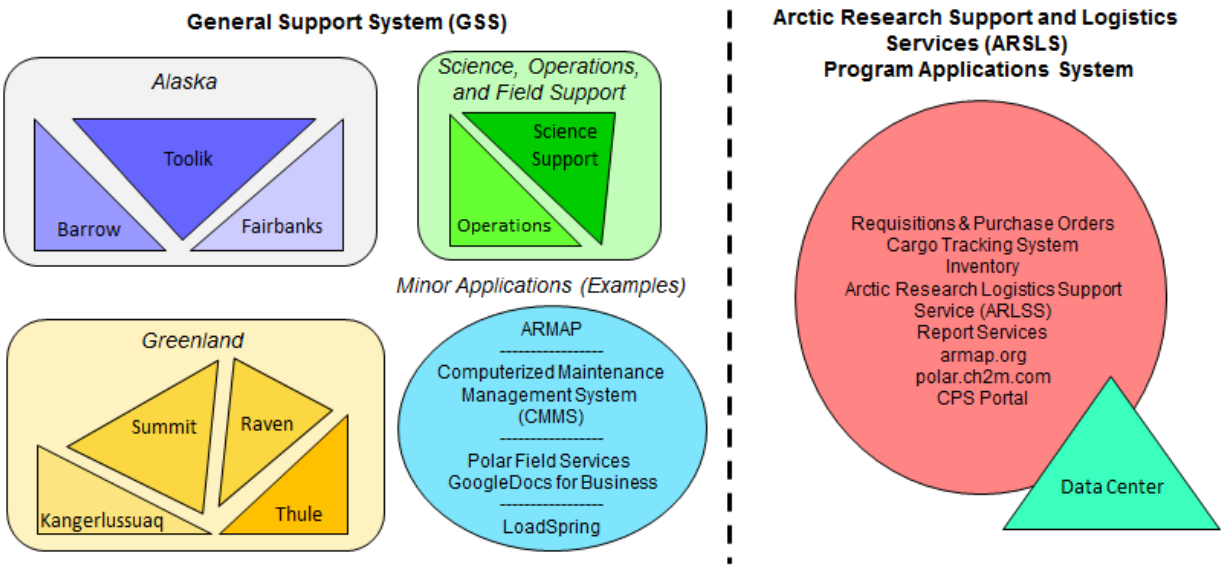

Figure 1. ARC Authorization Boundaries

Arctic Sciences Section General Support System

The ARC General Support System (GSS) is a set of interdependent information resources that share the common functionality of providing operational and science support to the ARC Program. The ARC GSS contains hardware, software, data, applications, communications, facilities, and people in three primary operating regions (Alaska, Greenland, Colorado) that support operation of the ARC Program. The GSS contains information systems that support operations and assets of the NSF ARC, including those provided or managed by partner agencies, contractors, grantees, or other sources. NSF assets include equipment that is acquired incidental to a Federal contract, cooperative agreement, or grant.

The GSS is categorized as a **Low** security threat to the ARC Program. This means that if there was a breach of confidentiality, integrity, or availability on a GSS system, the potential impact is expected to have a limited adverse effect on organization operation, organizational assets, or individuals.

Arctic Research Support and Logistics Services (ARSLS) Program Applications System

The one system of significance supporting the ARC Program is the Arctic Research Support and Logistics Services (ARSLS) Program Applications System. The ARSLS Program Applications System is comprised of multiple applications associated with a database containing information required to support research projects funded by the ARC Program. ARSLS Program applications disseminate information to personnel supporting funded research projects, the science community, and the general public.

The ARSLS Program Applications System is categorized as a **Moderate** security threat to the ARC Program. This means that if there was a breach of confidentiality, integrity, or availability on an ARSLS Program Applications System, the potential impact is expected to have a serious adverse effect on organization operation, organizational assets, or individuals.

For more information on the categorization of Arctic systems refer to the GSS or ARSLS Program Applications System Information Categorization and Sensitivity Assessment (ICSA).

Information Security Documentation

Documentation referenced throughout this handbook is developed and maintained in support of Federal requirements, NIST guidance, NSF policy, and ARC Program policies. The hierarchy of the ARC Program information security documentation taxonomy is depicted in Figure 2.

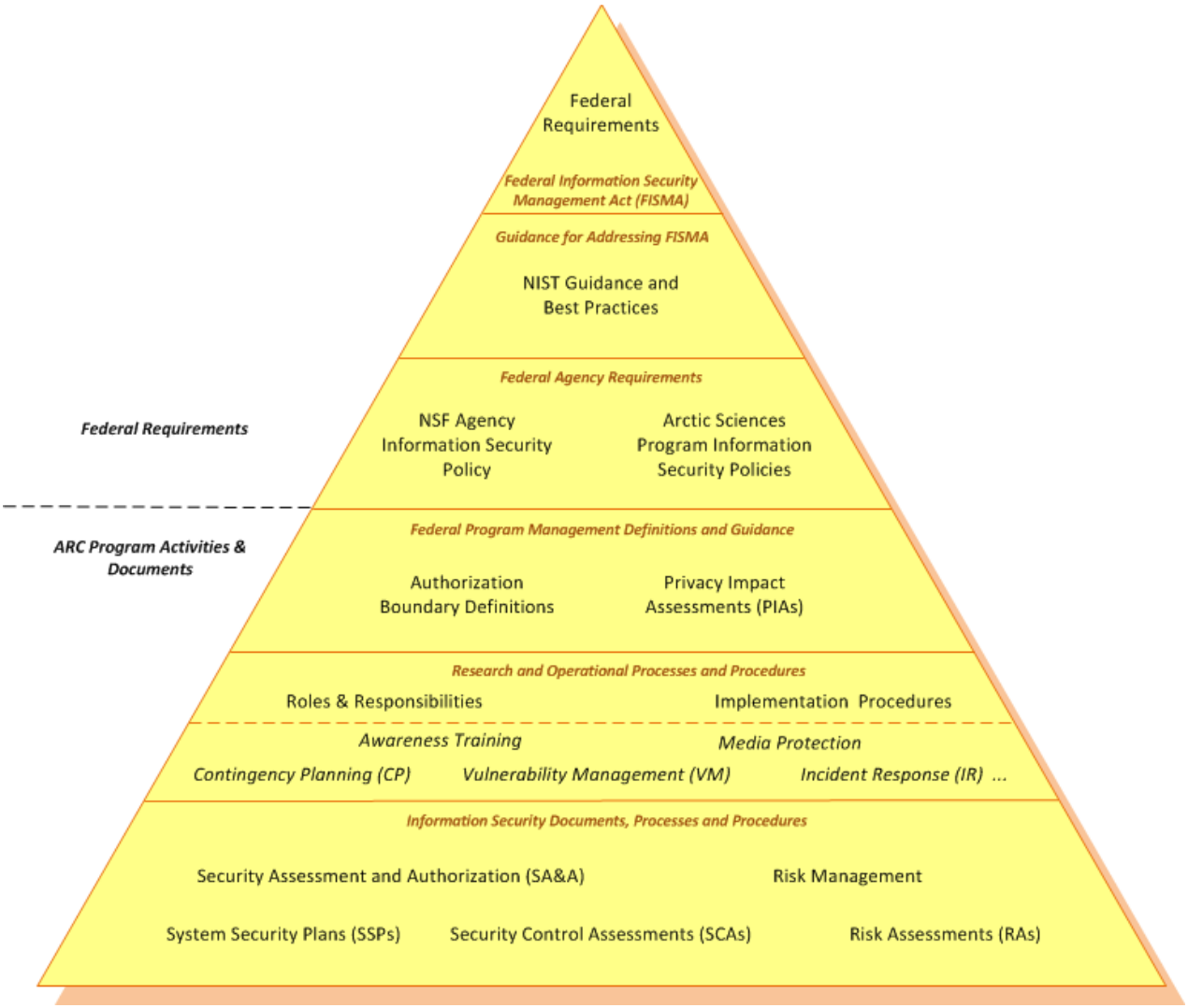

Figure 2. ARC Program Information Security Documentation Structure

As shown in Figure 2, ARC Program information security activities and documentation, depicted at the bottom of the pyramid, are driven by Federal requirements passed down through the NSF Agency to the program level. Specifically, the *Authorization Boundaries Definition* is used by the ARC Program to inform the NSF Agency of the systems managed by the program. *Privacy Impact Assessments (PIAs)* are also provided by the ARC Program to the NSF Agency to ensure compliance with Federal laws applicable to managing Personally Identifiable Information (PII).

Chapter II. Management Control Policies

Management control policies focus on administration of IT systems and the management of risk. Management controls are organizations, policies, and procedures used to reasonably ensure that (1) programs achieve their intended results, (2) resources are used consistent with program mission, (3) programs and resources are protected from waste, fraud, and mismanagement, (4) laws and regulations are followed, and (5) reliable and timely information is obtained, maintained, reported, and used for decision-making.

This section establishes ARC Program policies for:

- Planning
- Risk Assessment
    - Security Assessment and Authorization
    - Vulnerability Management

As ARC Program sites vary in management processes, physical layout and operational need, site specific implementations and deviations from policy requirements are documented in site specific procedures and System Security Plans (SSPs).

Planning

Responsibility: Agency

Planning policy requirements for Low and Moderate systems include:

- Develop, maintain, and implement a System Security Plan (SSP) for the general support system (GSS) and key applications in the ARC Program.
- Review and update SSPs annually to reflect changes to information systems and the environment of operation, as well as address vulnerabilities identified by risk assessments and security control assessments.
- Maintain and distribute an *ARC Program Information Security Rules of Behavior* to all ARC Program end users that describes responsibilities and expected rules of behavior with regard to information and information system usage, and receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

Additional planning policy requirements for Moderate systems only include:

- Coordinate security-related activities affecting information systems before conducting such activities in order to reduce impact on operations, assets, and individuals. Examples of security-related activities include security control assessments, risk assessments, contingency plan testing, vulnerability scanning, audits, remediation activities, and hardware and software maintenance.

Risk Management/Risk Assessment

The ARC Program manages risk in accordance with Risk Assessment control implementation guidance provided in NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information System and Organizations*, which defines information security risk as a measurement of the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. The following sections detail ARC program policy for assessing risk, documenting known system security status including known risk, and tracking known risk items for mitigation, remediation, and closure.

System Security Plans

Responsibility: Agency, Contractor

The ARC Program has a documented system security plan (SSP) for each general support system (GSS) and identified key applications (i.e. ARSLs) under its control, as defined by ARC Program Authorization Boundaries, as depicted in *Figure 1: ARC Program Authorization Boundaries*. ARC Program SSPs identify the current status of management, operational, and technical controls as identified in periodic reviews of security controls.

Security plans are living, dynamic documents reflecting the current information security posture of the ARC Program. In addition, the SSPs provide action plans and target dates for implementing controls where information security weaknesses have been identified. Further, the plans ensure that management and users of systems within the ARC Program are aware of their responsibilities and expected behavior with respect to access to ARC Program systems, information, and resources.

Security Assessment and Authorization

Responsibility: Agency, Contractor

Vulnerabilities are flaws or weaknesses that may allow harm to occur to an information system. In the ARC Program, vulnerabilities are often discovered during a regular review process known as Security Assessment.

ARC Program Security Assessment and Authorization (SA&A) processes align with the Risk Management Framework (RMF) presented in NIST SP 800-37 Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems.

The SA&A process required for Low and Moderate systems includes the following activities:

- *Categorize* the information system and information processed, stored, and transmitted by that system.
- *Select* an initial set of baseline security controls based on the security categorization; tailoring and supplementing the security control baseline as needed based on organizational assessment of risk and local conditions.
- *Implement* security controls and describe how controls are employed within the system and its environment.
- *Assess* security controls using appropriate assessment procedures to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements.
- *Assess* information system connections in the case of dedicated connections between information systems to determine requirements for Interconnection Security Agreements, and requirements for contracts, cooperative agreements, and grants.
- *Authorize* information system operation based on determination of the risk to organizational operations, assets, and individuals, resulting from the operation of systems and the decision of acceptable risk.
- *Monitor* security controls in the information system on an ongoing basis including assessing control effectiveness, documenting system or environmental changes, conducting security impact analyses of the associated changes, and reporting security state to program managers.

All known points of risk discovered during Security Assessment activities and related mitigation activities are tracked in the ARC Vulnerability Remediation Action Tracker (VRAT) which is governed by policy and procedure as addressed in the following section.

Vulnerability Management

Responsibility: Agency, Contractor

ARC Program Vulnerability and Risk Management processes align with the Risk Management Framework (RMF) presented in NIST SP 800-37 Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems.*

The ARC program assesses risk through Risk Assessments, Security Control Assessments, and/or Continuous Monitoring Activities as defined in the above sections. All known points of risk and related mitigations are then tracked in the ARC Vulnerability Remediation Action Tracker (VRAT). The VRAT provides a means of risk management implementation for the program, ongoing process of assessing the risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

The Arctic program VRAT serves to facilitate management processes that identify security weaknesses in the ARC program and outlines recommendations and milestones necessary for mitigation. Management of the VRAT, and thus program risk management, is conducted according to the ARC VRAT Management Process (Appendix D). This Process provides formal guidance to facilitate the remediation of ARC program- and system-level weaknesses, and provides a means for:

- Planning and monitoring corrective actions;
- Defining roles and responsibilities for weakness resolution;
- Assist in identifying funding requirements necessary to mitigate weaknesses;
- Tracking and prioritizing resources;
- Informing Arctic Program Research Science and Logistics (RSL) Program Managers (PMs); and
- Ensuring decision makers have a regularly scheduled opportunity to review VRAT items.

In addition to the quarterly VRAT management updates provided to RSL PMs, real time information regarding VRAT management is available on an ARC security team SharePoint site and can be accessed upon request by contacting the ARC Security team. All process information, record storage information, and details on the ARC Risk Management policy are fully defined in the ARC VRAT Management Process.

Chapter III: Operational Control Policies

Operational control policies address security methods focusing on mechanisms implemented and executed by people, as opposed to systems. These requirements improve security of a particular system (or group of systems), often require technical or specialized expertise, and may rely upon management activities as well as technical controls.

As ARC Program sites vary in management processes, physical layout and operational need, site specific implementations and deviations from policy requirements are documented in site specific procedures and System Security Plans (SSPs).

Personnel Security

Responsibility: Contractor

Personnel security involves the technical and administrative safeguards employed by personnel that use systems, including end users, software designers, operational technicians and managers. A broad range of security requirements related to the manner in which individuals interact with, receive access, and authorization to the information and the information systems they need to do their job.

An effective personnel security program includes (1) staffing procedures, (2) personnel screening, (3) segregation of duties, (4) system access procedures, (5) system user account management, and (6) security awareness training.

Definitions

- *Confidentiality* refers to the non-disclosure of information, directly or indirectly, to unauthorized person(s).
- *Least privilege* refers to the security objective of granting users only those accesses they need to perform their official duties.
- *Sensitive information* refers to information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information improper use of which could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act.
- *Segregation of duties* refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process.

Requirements

Personnel security policy requirements for Low and Moderate systems include:

- *Information retrieval upon termination* - Upon notification of termination or removal of personnel or participant, terminate information access, retrieve all information system-related property or media, and ensure appropriate retention or disposition of any records assigned to that employee or contractor.
- *Transfer upon reassignment* - Ensure that personnel or participant transfer actions result in appropriate reassignment of information system roles and responsibilities and information access consistent with the new position description and job function(s).
- *Access prerequisites* - Prior to receiving system access, personnel and participants must complete ARC Program Information Security Awareness Training.
- *Contract language* - Ensure third-party personnel security requirements, including roles and

responsibilities, are included in all contracts, or other agreements that bind ARC Program and any non-Arctic party in an agreement.

- *Authorization* - Request for system access by a user requires approval from the system manager.
- *Account request* - System operations staff members use the account request to create a user account for a new user. The user account provides only the system access that is approved for that individual based on their job requirements.
- *Access termination* - As soon as it becomes known that user accounts will no longer be required or that support personnel will no longer be employed in support of the ARC Program, the required documentation must be completed and the appropriate personnel notified to terminate access accounts.
- *Personnel Screening*- Ensure employees and contractors undergo background screening appropriate for the position they hold per NSF Manual 14, Personnel Manual. The Contractor Onboarding and Separation Guide documents the process to ensure contractors are permitted access only after appropriate background investigations have been completed.

Physical and Environmental Protection

Responsibility: Contractor

The following controls are strongly recommended for facilities housing computer resources supporting Low and Moderate systems. They may be tailored by environment as facilities range from purpose designed CONUS facilities to field locations.

Physical security and environmental security protections include measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. Effective physical security and environmental requirements address (1) physical access, (2) fire safety, (3) supporting utilities, (4) interception of data, and (5) mobile and portable systems.

Definitions

- *Computer resource* refers to something needed to support computer operations, such as hardware, software, data, telecommunications services, computer supplies, and other resources.
- *Environmental controls* are a subset of physical access controls that prevent or mitigate damage to facilities and interruptions in service. Smoke detectors, fire alarms and extinguishers, and uninterruptible power sources are some examples of environmental controls.
- *Library* refers to the physical site where magnetic media, such as magnetic tape, is stored.
- *Physical access* control refers to the type of control that involves restricting physical access to computer resources and protecting these resources from intentional or unintentional loss or impairment.
- *Proprietary* refers to privately owned, privately developed technology or specifications that the owner declines to divulge, thus preventing others from duplicating a product or program unless an explicit license is purchased.

Physical Access

The following controls are required for facilities housing computer resources supporting Low and Moderate systems:

- *Facility protections* - Where feasible, control access to the facilities through the use of guards, identification badges, or entry devices such as key cards.
- *Access review* - Regularly review the list of persons with physical access to sensitive facilities.
- *Authorizing media transfer* - Authorize and log the deposits and withdrawals of tapes and other storage media from media libraries and storage areas.
- *Locks* - Require keys or other devices for entry into the computer room or tape/media library. All unused keys or other entry devices should be secured from unauthorized access.
- *Visitors* - Ensure that visitors, contractors, and maintenance personnel are authenticated via appointments and ID checks. Require sign-in and escort of visitors to sensitive areas.

  When visitors who require an escort are present, sensitive information shall be protected from observation, disclosure, and removal. This includes storing or covering up documents and positioning computer monitors to prevent viewing by unauthorized persons.
- *Challenging authorization* - Visitors and permanently assigned personnel, regardless of position, shall be subject to challenge by other ARC Program personnel, facility physical security personnel.
- *Unusual activity* - Monitor physical accesses, review any unauthorized, unusual, or sensitive access activity, and take any remedial action, as necessary. Any violations should be reported to management.
- *Revoking access* - Ensure that physical access authorizations for personnel are revoked within 24 hours of a determination that physical access is no longer required.
- *Protecting systems and information* - Ensure that physical access to information systems are properly controlled based on the sensitivity of information.
- *Visitor access records management* - Authorized hosting facility operators shall maintain visitor access records to facilities under their management where ARC Program information systems reside (except for those areas within the facility officially designated as publicly accessible), which includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization shall review the visitor access records regularly.

Fire Safety

The following fire safety controls are required for facilities housing computer resources supporting Low and Moderate systems:

- *Detection and notification* - ARC Program facilities shall employ fire detection devices/systems that activate automatically in the event of a fire and, where appropriate, notify organization and emergency responders in the event of a fire.
- *Suppression and notification* - ARC Program facilities shall employ fire suppression devices/systems that provide notification of activation to the organization and emergency responders where feasible. ARC Program facilities shall employ an automatic fire suppression capability in facilities that are not staffed on a continuous basis.
- *Inspections* - The ARC Program ensures hosting facilities undergo fire marshal inspections and promptly resolve identified deficiencies.

Hosting Facilities

The following physical and environmental protections are required of hosting facilities for Low and

Moderate systems:

- *Authorization* - Hosting facilities shall be identified, evaluated and approved as authorized for operation with explicit written authorization by ARC Program Managers.
- *Locating systems* - At each ARC Program site, information systems must be located in an authorized hosting facility; primary or alternate.
- *Evaluation criteria* - Ensure that evaluation criteria include, but are not limited to: geography; geology; climate; availability, diversity and redundancy of communications services; availability, diversity, and redundancy of main power; education, availability, and sustainability of workforce; operational service levels; categorizations of information systems to be hosted within the facility; and proximity to other authorized hosting facilities.
- *Temperature and humidity* – Hosting facilities must maintain temperature and humidity levels where information systems reside, and monitor temperature and humidity levels. Specifically, hosting facilities are required to employ automatic temperature and humidity controls to prevent fluctuations potentially harmful to the information system, and monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.
- *Water protections* – Hosting facilities must have automated mechanisms that, without the need for manual intervention, protect the system from water damage in the event of a water leak. Hosting facilities must protect information systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

Supporting Utilities

The following controls over supporting utilities are required for facilities housing computer resources supporting Low and Moderate systems:

- *Heating and air conditioning* - Regularly maintain heating and air-conditioning.
- *Monitoring utilities* - Periodically review electric power distribution, heating plants, water, sewage, and other utilities for risk of failure.
- *Plumbing* - Ensure that the locations of building plumbing lines are known and do not endanger systems.
- *Backup power* - Provide an uninterruptible power supply (UPS) or backup generator where appropriate

Interception of Data

The following controls to prevent the interception of data are required for facilities housing computer resources supporting Low and Moderate systems:

- *Physical access* - Ensure that physical access to communications infrastructure is limited to authorized personnel and physically secured. At a minimum:
    - Control physical access to data transmission lines as appropriate.
    - Unused or spare cable connection points shall be physically disconnected from active information technology equipment; and
    - Physical low-voltage cabling installations shall comply with industry best practices and standards current at the time of installation (and not the time of design).
    - Physical access to information system devices that display information shall be controlled to prevent unauthorized individuals from observing the display output.

Mobile and Portable Devices

The following controls over mobile and portable devices are required for facilities housing computer resources supporting Low and Moderate systems:

- *Protecting against disclosure* - Encrypt sensitive data on mobile devices as a precaution against the potential disclosure of information if the device is lost or stolen. Any sensitive media stored on electronic media shall be encrypted using FIPS 140-2 *Security Requirements for Cryptographic Modules* compliant encryption.
- *Storage* - Arctic personnel should securely store portable devices when not in use.

Hardware and System Software Maintenance

Responsibility: Contractor

This section provides requirements for routine and preventative maintenance of information systems. Requirements pertain to how maintenance is approved, scheduled, performed, documented, reviewed, and validated.

- *Hardware* is the physical components of information technology, including the computers, peripheral devices such as printers, disks, and cables, switches, and other elements of the telecommunications infrastructure.
- *System software* is the set of computer programs and related routines designed to operate and control the processing activities of computer equipment. It includes the operating system, utility programs, and security software and is distinguished from application software.
- *Resource availability* - Ensure that resources are available to production users to the maximum extent practicable, and that costs to the Government due to system unavailability, equipment malfunctions and failures, and other outages are minimized.
- *Routine activities* - To ensure adequate controls over hardware and system software, (1) limit access to hardware and system software, (2) review, test, and authorize system software and hardware prior to implementation, (3) manage systems to reduce vulnerabilities.
- *Local maintenance and diagnostic activities* - Conducted by individuals physically present at the information system, not communicating across a network connection.
- *Non-local maintenance and diagnostic activities* - Conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network.

Management of Systems to Reduce Vulnerabilities

- Ensure that systems are periodically reviewed to identify and, eliminate unnecessary services (e.g., FTP, HTTP, etc.).
- Systems should periodically reviewed for known vulnerabilities and software patches, if needed, should be properly installed.

Controlled Maintenance

Controlled maintenance of Low and Moderate systems requires:

- Maintenance activities to be scheduled, performed, documented, and reviewed records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications

- Control over all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
- Designated official explicit approval for the removal of the information system or system components from facilities for off-site maintenance or repairs;
- Sanitizing of equipment to remove all information from associated media prior to removal from facilities for off-site maintenance or repairs; and
- Checking all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

Moderate systems also require:

- Maintenance records to include date and time of maintenance; name of the individual performing the maintenance; name of escort, if necessary; a description of the maintenance performed; and a list of equipment removed or replaced (including identification numbers, if applicable).
- The approved and monitored use of tools such as, diagnostic and test equipment used to conduct maintenance on the information system. Media containing diagnostic and test programs must be checked for malicious code before the media is used on the system.

Non-Local Maintenance

Non-local maintenance and diagnostic activities for Low and Moderate systems require:

- Activities to be authorized, monitored, and controlled
- Allow the use of maintenance and diagnostic tools only as consistent with approved ARC policy and operational IT procedures.
- Strong identification and authentication techniques in the establishment of non-local sessions, such as the use of PKI where certificates are stored on a token protected by a password, passphrase, or biometric.
- Maintained records for all activities
- Termination of all sessions and network connections when maintenance is complete

Requirements for Moderate systems only:

- Audit non-local maintenance and diagnostic sessions, and designate personnel to review records of the sessions
- Document the installation and use of non-local maintenance and diagnostic connections in the system security plan

Maintenance Personnel

Maintenance personnel activities for Low and Moderate systems require:

- Establish a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel.
- Ensure personnel performing maintenance on the system have required access authorizations, or designate personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.
- Based on a prior assessment of risk temporary credentials may be issued for one-time use or for a very limited time period when an individual, such as a vendor or subcontractor, not previously identified in the system legitimately requires privileged access to the system, for example, when required to conduct maintenance or diagnostic activities with little or no

notice.

Timely Maintenance

Moderate systems require maintenance support and/or spare parts for IT and security-critical components of the system to be obtained within a pre-defined acceptable time period of failure.

Specify the information system components that, when not operational, result in increased risk because the security functionality intended by that component is not being provided. Security-critical components include, for example, firewalls, intrusion detection systems, audit repositories, and authentication servers.

Media Protection

Responsibility: Contractor

Media protection policies are required to protect ARC Program information systems and data through the secure use, storage, protection, transportation and disposition of all media that stores data or information.

Definitions

- *Computer media* refers to resources related to input or output data processing, such as tapes, disks, external hard drives, thumb drives or hard copy.
- *Input controls* refer to safeguards applied to the information entered into a computer or during the process of entering data into the computer.
- *Output controls* refers to the controls over the data/information produced by computer processing, such as a graphical display on a terminal or a hard copy document.
- *Production environment* refers to the system environment where the ARC Program performs its operational information processing activities.
- *Controlled Areas* are any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.
- *Disposal* is the act of discarding media with no other sanitation considerations.
- *Clearing* is a media sanitization method that protects the confidentiality of information by not allowing retrieval by data, disk or file recovery utilities. One method for clearing media that is writeable and has not been damaged is overwriting sensitive data with non-sensitive/random data.[2]
- *Purging* is a media sanitization method that is more extensive than clearing which can be achieved for magnetic media by degaussing, which destroys the media on which the data is stored. In order to purge data from non-magnetic media, the media must be destroyed, which can be accomplished by disintegration, incineration, pulverizing, shredding, or melting.

Requirements

To adequately support the operations of ARC Program information systems in a production environment, effective user support and adequate controls over media are required.

[2] For recommendations on suitable products for data clearing and purging refer to NIST SP 800-36, *Guide to Selecting Information Security Products*.

Access

Media access requirements apply to Low and Moderate systems:

- *Authorized use* - All digital and non-digital media associated with ARC Program information systems is restricted to authorized users through manual and/or automated means.

Protection

Media protection requirements apply to Low and Moderate systems:

- *Sensitive information* - All media containing Medical Information, Personally Identifiable Information (PII) and Sensitive Information (SI) must be protected during use, storage, transport, sanitization and disposal. All types of removable media containing these types of information must be approved for removal from the system, and encrypted when in digital format.
- *Encryption* - Any PII or SI stored on electronic media shall be encrypted using FIPS 140-2 *Security Requirements for Cryptographic Modules* compliant encryption. The decryption key shall be transported separately, or transmitted via an alternate channel of communication.
- *Inactive media* - Ensure that all equipment/media not in active use are secured at all times. This shall be in an office with controlled/locked access, and under direct control of a designated individual(s).

Transportation

Media transport requirements only apply to Moderate systems:

- *Outside of controlled areas* - Only authorized personnel are allowed to transport or ship digital and non-digital media outside of ARC Program controlled areas. Accountability must be maintained on any media transported outside of a controlled area.
- *Authorization* - Only personnel authorized in writing to do so shall transfer, pickup, or deliver sensitive media. A written log shall be kept recording the transfer, pick up, and delivery of sensitive media affiliated with the ARC Program.
- *Chain of custody* - Transportation of sensitive equipment and/or media shall require hand delivery with receipts documenting chain of custody and control, or, if shipped via common carrier, require tracking and signature upon delivery.

Labeling

Media labeling requirements only apply to Moderate systems:

All removable information system media must be labeled in accordance with ARC Program instructions. Removable or portable digital media that contain PII and/or SI data shall be labeled as follows:

> **WARNING: NSF ARC Program Protected Information; misuse can result in criminal and civil penalties.**
>
> **Information/Data Sensitivity:** MODERATE
>
> **Date:** *<<MM/DD/YYYY>>*
>
> **Information Owner: <<** *Include the full name, organization, telephone number, and email address of the information owner. >>*

Sanitization

Media sanitization requirements apply to Low and Moderate systems. All information system media must be sanitized prior to disposal or release for reuse. Non-digital media that contain SI/PII must be physically destroyed, which can be accomplished by disintegration, incineration, pulverizing, shredding or degaussing according to NSA regulations.

Digital media containing data or information that does not contain PII or SI must be cleared using an approved application or tool. Digital media containing data or information that does contain PII or SI must be purged using an approved application or tool. Where such an application is not available, purging shall consist of demagnetizing or destroying the media in a manner that prevents recovery of the information.

Contingency Planning

Responsibility: Contractor

Contingency planning addresses how to keep ARC Program critical functions operating in the event of disruptions, large and small. The purpose of a contingency plan is to minimize the loss of critical assets and information resources in the event of a disaster and ensure the continuation of critical operations and services. Contingency plans must be documented, tested, and updated at least annually throughout the system life cycle, and formally approved by a designated official.

Effective contingency planning includes the following: (1) identification of the most critical and sensitive operations and resources, (2) assignment of responsibility, (3) training, (4) restoration of operations, (5) periodic testing, and (6) offsite facilities.

Each Arctic site must develop a contingency plan for the infrastructure and systems under its control. The contingency plan must include contingency procedures for all infrastructure, systems, and applications supported by the relevant segment of the GSS authorization boundary.

Definitions

- *Contingency plan* is the management policy and procedures designed to maintain or restore business and computer operations, possibly at an alternate location, in the event of an emergency, system failure, or disaster. The three critical elements of a contingency plan are:
    - Identification of the most critical and sensitive operations and their supporting computer resources.
    - Documentation.
    - In place and tested contingency/disaster recovery plans.
- *Contingency planning* includes interim measures taken to recover IT services after an emergency or system disruption. Contingency planning is also sometimes referred to as disaster recovery, business continuity, continuity of operations, or business resumption planning. Interim measures may include the relocation of IT systems and operations to an alternate site, recovery of IT functions using alternate equipment, or performance of IT functions using manual methods.
- *Emergency procedures* are response procedures for occupants of a facility in the event of a situation posing a potential threat to the health and safety of personnel, the environment, or property. Emergency procedures are developed at the facility level, specific to the geographic location and structural design of the building.

Requirements

Contingency planning requirements apply to Low and Moderate systems:

- *Disaster response* - The contingency plan shall focus on location relevant disasters, or system failures, and how to respond in the event that a disaster occurs.
- *Distribution* - Contingency plans shall be distributed to all key contingency personnel and be continuously updated to reflect changes in personnel, role, and function.
- *Testing* - The contingency plan, including emergency procedures and offsite processing, should be fully tested on an annual basis, and adjusted as appropriate.
- *Maintenance* - Maintain current inventory lists, software license information, and/or vendor contact lists, as supporting documentation to the contingency plan.

Backup and Recovery

Backup and recovery requirements apply to Low and Moderate systems. Incorporate backup strategies for critical assets into existing backup processes, which include recurring backup and recovery procedures specific to their environment. Ensure that backups conform to the following best practice procedures and are routinely tested for verification:

- Label the backup media.
- Adequately and systematically backup all data, operating systems, and utility files, including all system state, patches, fixes, and updates.
- Maintain complete records of what data is backed up, how it is labeled, and where it is stored, including off-site storage locations.
- Maintain backups of software licensing records.
- Store copies of the back-up media including the back-up record safely in a remote location, at a sufficient distance away to escape any damage from a disaster at the main site.
- Perform periodic tests of restoring data/software from the backup copies to ensure that they can be relied upon for use in an emergency.
- Ensure that backup information is tested at least annually to ensure media reliability and information integrity.

Security Awareness and Training

Responsibility: Agency

People are a crucial factor in ensuring the security of program systems and valuable information resources. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge.

Definitions

- *Security awareness* includes materials such as presentations, posters, banners, newsletters, and activities such as security awareness days that are used to focus attention on information security concerns and appropriate responses to information security incidents.

Information Security Awareness Training

Awareness training requirements apply to both ARC Low and Moderate systems and is designed to ensure general security awareness and training is provided to all personnel and participants, and training completion records are documented before authorizing access to ARC IT resources. Training must be completed by those with access to ARC IT resources on an annual basis. Training shall be composed of relevant and needed security skills and competencies to facilitate job performance, and to focus attention on security, and to change behavior or reinforce good security practices.

Training shall be completed soon after initiating participation in or employment in support of the ARC Program. All ARC Program users shall complete an annual security training program to refresh/increase their knowledge of information security.

Incident Response

Responsibility: Agency, Contractor

Any activity that is a threat to the confidentiality, integrity, or availability of information resources, has the potential to undermine science or operational activities, presents legal issues related to sensitive data, or is a misuse of government information resources is considered an incident. Examples of incidents include the presence of viruses or other malicious software; network probes, attacks or penetration; denial of service, the assumption of control of an information resource by an unknown or unauthorized user, or the breach of sensitive or Personally Identifiable Information (PII)[3].

ARC Program incident response (IR) establishes processes and tools that effectively identify and detect incidents, evaluate the threat, report incident specifics appropriately, implement corrective action, capture lessons learned, and close out the incident. This section provides requirements for incident handling and determining the appropriate response.

Incident response control requirements apply to Low and Moderate systems.

Incident Response Planning

ARC IT and Communications (IT&C) service providers collaborate with the ARC Information Security Team and ARC RSL Program Managers (PMs) to establish processes and tools that effectively identify and detect incidents, evaluate the threat, report incident specifics appropriately, implement corrective action, capture lessons learned, and close out the incident.

The IR Plan tailored for the ARC-program addresses:

- Defining the categories of reportable incidents and the time period in which suspected incidents are to be escalated or notified to those identified as responsible for providing guidance on and for managing the incident
- Developing and disseminating procedures for performing incident handling and reporting, based on the IR policy and IR Plan
- Selecting a team structure and staffing model for responding to potential incidents
- Determining what services the incident response team should provide
- Setting guidelines for communicating with service providers or outside parties regarding incidents
- Training potential incident response team members
- Coordinating incident handling and contingency planning activities
- Incorporating lessons learned from ongoing incident handling activities into incident response procedures and training

The ARC Incident Response Plan (Appendix C) addresses incident identification, handling, response, and notification policy and procedure for ARC program IT&C service providers, contractors, grantees,

[3] For guidance on responding to a suspected PII breach refer to *Privacy Specific Security Measures, Privacy Incident Response* in Chapter IV: Privacy Policies.

and teaming partners governed by cooperative agreement. The plan expands upon the policy provided in this handbook to address specific procedures for all staff who support the ARC program and provides relevant templates and contract information to adequately conduct Incident Response in accordance with this policy and includes guidelines for evidence handling as well as incident reporting.

Chapter IV: Privacy Policies

This chapter provides the minimum requirements for implementing effective protections to ensure privacy of sensitive information. This guidance applies to all ARC Program participants involved in the creation, use, maintenance, and disposal of sensitive information, including personally identifiable information (PII).

Personnel, contractors, subcontractors, service providers, and participants who access sensitive data managed by or on behalf of the ARC Program are responsible for avoiding inappropriate access, use, or disclosure. Effective privacy for individuals depends on a solid foundation of information security safeguards in the information systems that process, store, and transmit PII. Note that privacy is more than security and confidentiality and includes the principles of transparency, notice, and choice.

ARC Program privacy guidance is based on the Fair Information Practice Principles (FIPPs) embodied in the Privacy Act of 1974, the EGovernment Act of 2002 (Section 208), and related Office of Management and Budget (OMB) guidance[4]. The ARC Program monitors federal privacy laws and policy for changes that affect the privacy program, and updates policy and procedures as required.

Privacy of Sensitive Information

Those supporting the ARC Program may, in the course of performing their official duties, have a wide variety of sensitive information about individuals available to them electronically and in hard copy. Sensitive data includes PII, financial information such as bank account numbers, reviews, reviewer identity tied to reviews, unfunded proposals, proprietary parts of funded proposals, and other similar information. Although the majority of sensitive information maintained by the ARC Program is in an NSF systems of records protected under the Privacy Act such as proposal jackets, personnel files, Principal Investigator and Reviewer files, sensitive data may also exist in other types of records, such as databases, log files, e-mail, and correspondence files.

Medical Information is protected health information that can be associated with an individual. Contractors, subcontractors, and service providers supporting the ARC Program who have access to medical information are responsible for managing and handling medical information in compliance with Health Insurance Portability and Accountability Act (HIPAA) regulations. These Federal regulations are designed to protect the privacy of individuals requiring medical attention while allowing sharing of health information to promote public health.

Personally Identifiable Information (PII) is any information about an individual including: (i) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (ii) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Sensitive Information (SI) refers to information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use could adversely affect the ability of an ARC Program to accomplish its mission, proprietary information, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act.

[4] The ARC Program definition of PII is in accordance with OMB Memorandum M-07-16 *Safeguarding Against and Responding to the Breach of Personally Identifiable Information, and* NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*.

Transparency

The ARC Program addresses requirements for transparency by providing effective notice to the public and individuals regarding ARC Program collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII), including the authority the ARC Program has for collecting PII. Privacy Act Statements are included on or referenced by forms used to collect PII. Notices to the public are provided at the point of collection and include details regarding:

- How PII is protected.
- How individuals may obtain access to PII for the purpose of having it amended or corrected.
- Choices individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices.
- Details on the PII being collected and maintained by the ARC program, the purpose for which the information is collected, how the information is used, and if applicable shared with external entities and for what purpose.
- Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise such consent.

When there are changes in practice or policy affecting PII or impact privacy, public notices are revised to reflect the change and made available to the public. Dissemination of public notices ensures that individuals are aware of and when feasible, consent to all uses of their PII by the ARC Program.

The ARC Program also maintains transparency of privacy activities by ensuring that the public has access to information about ARC Program privacy practices, avenues for communicating with privacy officials, and by contributing to NSF Agency published Privacy Impact Assessments (PIAs) and System of Records and Notice (SORNs).

Individual Participation and Redress

The ARC Program involves individuals in the decision making process regarding the collection and use of their PII. To address this requirement, the ARC Program where feasible, provides the means for individuals to authorize the collection, use, maintenance, and sharing of their PII prior to collection. This authorization process also informs individuals of the consequences of approving or declining the authorization of collection, use, dissemination, and retention of PII. When there is a Program need to use previously collected PII for another purpose, where feasible and appropriate consent from the individual is obtained prior to use.

The ARC Program provides individuals the ability to have access to their PII maintained in its system(s) of records in order to determine whether to have the PII corrected or amended, as appropriate. The Program also provides a process for individuals to have inaccurate PII maintained by the ARC Program corrected or amended, as appropriate; and establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information sharing partners, and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

The ARC Program process of involving individuals in the management of their PII also includes providing individuals with a venue for receiving and responding to complaints, concerns, or questions from individuals about ARC Program privacy practices. Complaints, concerns, or questions should first be addressed to the individuals contracting organization, and may be escalated to the ARC Information Security Team if concerns remain unaddressed. Though immediate resolution may not always be possible, the ARC Information Security team will endeavor to address any escalated PII inquiries within one month.

Authority and Purpose

The ARC Program identifies the legal bases that authorize a particular PII collection or activity that impacts privacy; and specifies the purpose(s) for which PII is collected.

Authority activities include determining the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need. Before collecting PII in connection with an information system or program, the ARC Program determines whether the contemplated collection of PII is legally authorized. ARC Program Managers consult with the NSF legal counsel regarding the authority of any collection of PII.

Purpose activities include describing the purposes for which PII is collected, used, maintained, and shared in privacy notices; PIAs and SORNs maintained by the NSF Agency.

Access to PII/SI/MI

All ARC Program information systems that process, store, or transmit PII and/or other sensitive information are subject to the following access requirements.

- *Access authorization* - Enforce assigned authorizations for controlling access to systems.
- *Authentication control* - Utilize a properly maintained and configured authentication control as defined in current revisions of NIST SP 800-53/800-63.
- *Logging* – Log all access to applications and systems. Ensure that audit logs are accessible for review only by authorized security and system administration personnel.
- *Authorizing information flow* - Enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems and systems that contain PII and/or other sensitive information.
- *Prohibited sharing* - The use of non-Government external computing resources to access ARC Program computing resources that store, process, or transmit PII and/or other sensitive information is strictly prohibited unless approved in advance in writing.
- *Cryptography* - If cryptographic methodology (e.g., secret key and public key) is used, the product and the implementation methods should meet Federal standards (e.g., Data Encryption Standard, Digital Signature Standard).
- *Key management* - If encryption is used, separate procedures should be developed for key generation, distribution, storage, use, destruction, and archiving.
- *Transmission* - Any ARC Program sensitive, PII, proprietary, or private information shall not be sent via the Internet unless it has first been encrypted by approved methods.

Data Minimization and Retention

The ARC Program only collects, uses, and retains PII that is relevant and necessary for the specified purpose for which it was originally collected. The ARC Program retains PII for only as long as necessary to fulfill the specified purposes[5].

Minimization of PII

The ARC Program minimizes the collection, use and retention of PII by:

- Identifying the minimum PII elements (e.g., name, address, date of birth) relevant and

[5] Record retention practices are in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule.

necessary to accomplish the legally authorized purpose of collection.

- Limiting the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent.
- Conducting an initial evaluation and performing periodic evaluations of its holdings of PII to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.
- Where feasible and within the limits of technology, the ARC Program locates and removes or redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.
- PII gathered and maintained for the ARC Program is not authorized to be used for training or research purposes, or in testing of pre-deployment applications; commercial-off-the-shelf (COTS) applications or applications in development.

Data Retention and Disposal

The ARC Program:

- Retains PII for only as long as is necessary to fulfill the purpose(s) identified in the notice or as required by law.
- Appropriately disposes of PII when it is no longer necessary to retain it.
- Systematically destroys, erases, and/or anonymizes the PII, regardless of the method of storage (e.g., electronic, optical media, or paper-based) in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and
- Uses audits and appropriate technology to ensure secure deletion or destruction of PII, including originals, copies, and archived records.
- Where feasible, configures information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.

Use Limitation

In compliance with the Privacy Act, the ARC Program prohibits uses of PII that are either not specified in notices, incompatible with the specified purposes, or not otherwise permitted by law. Specifically, the ARC Program:

- Ensures that PII is only used for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or in its public notices. These steps include monitoring and auditing use of PII, and training personnel and participants on the authorized uses of PII.
- Shares PII with third parties, including other public and private sector entities, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or in a manner compatible with those purposes.
- Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically enumerate the purposes for which PII may be used.
- Monitors, audits, and trains its staff on the authorized uses and sharing of PII with third parties.

- Establishes and implements a process for evaluating any proposed new instances of sharing PII with third parties to assess whether they are authorized and whether additional or new public notice is required.
- Designs information systems to collect, use, maintain, and share PII only for the authorized purposes specified in the Privacy Act and/or organizational public notice(s) or for uses compatible with those purposes.

Data Quality and Integrity

ARC Program data quality and integrity measures enhance public confidence that any PII collected and maintained is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the public notice. The ARC Program takes the following steps to confirm accuracy of PII:

- Confirms to the extent feasible upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that PII.
- Collects PII directly from the individual to the greatest extent practical.
- Requests that the individual validate PII during the collection process and revalidate PII annually.
- Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems.
- Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.
- Where feasible, ARC systems are configured to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.
- Documents processes to ensure the integrity of PII through existing security controls.
- Establishes a Data Integrity Board when appropriate, to oversee organizational computer matching agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

Privacy Specific Security Measures

NSF's *Policy Regarding the Privacy of Sensitive Information* states that sensitive and/or PII must not be disclosed outside of NSF except as authorized by the Privacy Act. In coordination with security guidance and practices defined in this Handbook, additional security measures are implemented by the ARC Program to ensure administrative, technical, and physical measures are in place to protect PII collected or maintained by the ARC Program against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that planning and responses to privacy incidents comply with OMB policies and guidance. Allocation of resources to implement privacy measures is determined by ARC RSL Management.

Inventory of PII

In coordination with the maintenance of ARC Program Privacy Impact Assessments (PIAs), the ARC Program establishes, maintains, and regularly updates a PII inventory that contains a listing of all information systems identified as collecting, using, maintaining, or sharing PII; and provides updates to the NSF to support the establishment of appropriate information security requirements for all new or modified information systems containing PII.

PII inventory information is gathered by extracting the following information elements from PIAs of

information systems containing PII:

- name and acronym for each system identified
- types of PII contained in that system
- classification of level of sensitivity of all types of PII, as combined in that system
- classification of level of potential risk for damage to affected individuals and organizations if PII is exposed

Privacy Incident Response

Employees, contractors, subcontractors, Intergovernmental Personnel Act employees (IPAs), Visiting Scientists, Engineers, and Educators (VSEEs), and others are responsible for recognizing and safeguarding PII in the possession of the Federal Government, and preventing inappropriate access, use, or disclosure. In the event of a suspected or confirmed breach of PII all ARC Program participants must report the incident to their immediate supervisor and/or directly to ARC RSL PMs.

In the event of a suspected PII breach, the ARC Information Security Team and the IT&C service provider assess and share the information below with ARC RSL PMs. The response team documents and assesses the likely risk of harm caused by the breach: 1) nature of the data elements breached; 2) number of individuals affected; 3) likelihood the information is accessible and usable; 4) likelihood the breach may lead to harm; and 5) the ability of the ARC program to mitigate the risk of harm. ARC RSL PMs will evaluate suspected PII breach information to determine whether notification of a breach outside of the program is required.

If notification is recommended, ARC RSL PMs notify the NSF Chief Privacy Officer (CPO) to convene an NSF Privacy Incident Response Team (PIRT). The PIRT is responsible for responding to the loss of PII and assists in addressing and mitigating the risk of identity theft; initiating specific actions for recovery; determining incident reporting and handling requirements; and assessing where notification of affected persons or mitigation is reasonably required. The PIRT determines the appropriate level of response to the actual or potential breach to mitigate risk and harm, and initiates corrective action as required. For more information on NSF Agency incident response please refer to the *National Science Foundation, Computer Security Incident Response Plan.*

Accountability, Audit, and Risk Management

This section demonstrates ARC Program accountability for and commitment to the protection of individual privacy. Accountability, audit, and risk management policies are designed to enhance public confidence through effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the ARC Program is complying with all applicable privacy protection requirements and minimizing its overall privacy risk. Specifically the ARC Program:

- Develops, disseminates, and implements privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII.
- Develops a privacy plan for implementing applicable privacy controls, policies, and procedures.
- Updates privacy plan, policies, and procedures on an annual basis.
- Establishes a privacy risk assessment process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, and use of personally identifiable information.
- Conducts a Privacy Impact Assessment (PIA) for information systems and programs in accordance with OMB policy and NSF Agency policy and procedures, which include

documented, repeatable processes for conducting, reviewing, and approving PIAs.

ARC Program privacy risk assessment processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. Specific ARC Program privacy requirements for contractors, subcontractors, and service providers include to:

- Establish and monitor compliance of privacy requirements including privacy roles and responsibilities for contractors, subcontractors, and service providers.
- Include privacy requirements in contracts, subcontracts, and other acquisition-related documents.

Privacy Monitoring and Auditing

The ARC Program annually monitors and audits privacy practices in accordance with Federal privacy laws and policy, and internal privacy policy to ensure effective implementation. These monitoring activities identify and address gaps in privacy compliance, management, operational, and technical controls.

Accounting of Disclosures

The ARC Program consistent with, and subject to exceptions in the Privacy Act, supports the NSF Agency by:

- Maintaining accurate accounting of disclosures of information held in each system of records, including date, nature, and purpose of each disclosure of a record; and name and address of the person or agency to which the disclosure was made.
- Retaining the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer.
- Making the accounting of disclosures available to the person named in the record upon request.

Privacy Awareness Training and Rules of Behavior

The ARC Program develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures; and targeted, role-based training for personnel with significant PII responsibilities; and ensures that applicable personnel certify acceptance of responsibilities for privacy requirements.

ARC Program personnel assigned to work with sensitive information must review and sign rules of behavior, which detail the responsibilities of and expectations for all individuals with access to sensitive information, particularly personally identifiable information (PII).

Privacy Reporting

The ARC Program develops, disseminates, and updates reports to the NSF as required by the Agency for reporting to the Office of Management and Budget (OMB) and Congress to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

Appendix A: Glossary

Access is the ability to do something with a computer resource; use, change, or view.

Access control is the means by which access is explicitly enabled or restricted in some way, usually through physical and system-based controls.

Application means the use of information resources to satisfy a specific set of user requirements. Examples of applications include financial management systems, procurement systems, or personnel systems.

Authentication is the means of establishing the validity of a user's claimed identity to the system. There are three means of authenticating a user's identity which can be used alone or in combination: something the individual knows (a secret -- e.g., a password, Personal Identification Number (PIN), or cryptographic Key); something the individual possesses (a token -- e.g., an ATM card or a smart card); and something the individual is (biometrics -- e.g., characteristics such as a voice pattern, handwriting dynamics, or a fingerprint).

Baseline configuration is a documented, up-to-date specification to which the information system is built. This document provides details about the components of a system, for example the standard software installed on a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information. This document also provides applicable details on network topology and the logical placement of the component within the system architecture. Maintaining the baseline configuration involves creating new baselines as the information system changes over time.

Clearing is a media sanitization method that protects the confidentiality of information by not allowing retrieval by data, disk or file recovery utilities. One method for clearing media that is writeable and has not been damaged is overwriting sensitive data with non-sensitive/random data.[6]

Common controls are security controls that are inheritable by one or more information systems. The identification of common controls is most effectively accomplished as a Program-wide exercise with the active involvement of all IT stakeholders. Common control selection takes into consideration the security categories and associated impact levels of the information systems in accordance with FIPS 199 and FIPS 200, as well as the security controls necessary to adequately mitigate the risks arising from the use of those systems.

Computer media refers to resources related to input or output data processing, such as tapes, disks, external hard drives, thumb drives or hard copy.

Computer resource refers to something needed to support computer operations, such as hardware, software, data, telecommunications services, computer supplies, and other resources.

Confidentiality refers to the non-disclosure of information, directly or indirectly, to unauthorized person(s).

Contingency plan is the management policy and procedures designed to maintain or restore business and computer operations, possibly at an alternate location, in the event of an emergency, system failure, or disaster.

Controlled Areas are any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the

[6] For recommendations on suitable products for data clearing and purging refer to NIST SP 800-36, *Guide to Selecting Information Security Products*.

information and/or information system.

Data integrity is the property that data has when it has not been altered in an unauthorized manner.

Disposal is the act of discarding media with no other sanitation considerations.

Emergency procedures are response procedures for occupants of a facility in the event of a situation posing a potential threat to the health and safety of personnel, the environment, or property. Emergency procedures are developed at the facility level, specific to the geographic location and structural design of the building.

Environmental controls are a subset of physical access controls that prevent or mitigate damage to facilities and interruptions in service. Smoke detectors, fire alarms and extinguishers, and uninterruptible power sources are some examples of environmental controls.

General Support System[7] (GSS) is an interconnected set of centrally provided information resources under the same direct management control that share common functionality. A GSS typically includes hardware, software, information, data, applications, communications, and people. Direct management control refers to budgetary and operational authority for the day-to-day maintenance of the information systems. A GSS can be, for example, a mainframe or a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization.

Hardware is the physical components of information technology, including the computers, peripheral devices such as printers, disks, and cables, switches, and other elements of the telecommunications infrastructure.

Identification is the means by which a user provides a claimed identity to the system. The most common form of identification is the user ID.

Impact is the level of impact from a threat event is the magnitude of harm that can be expected to result from the unauthorized disclosure, modification, disruption, destruction, or loss of information and/or denial of service.

Information resources include both government information and information technology supporting the ARC Program mission.

Information Owner is the individual who has the operational authority in the ARC Program for specified information, and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal to ensure the confidentiality, integrity, and availability of that information.[8]

Information Manager is the individual(s) who has the operational responsibility for following operational procedures supporting established controls for the generation, collection, processing, dissemination, and disposal of specified information.

Information System is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial/process controls systems, telephone switching and

[7] As defined by OMB Circular A-130, Appendix III.

[8] The responsibilities of the information owner and manager are different than the responsibilities of the owner and manager of the system on which the information resides. The types of systems supporting the mission of the ARC Program are listed in the *ARC Program Information Systems* section provided earlier in this document.

private branch exchange (PBX) systems, and environmental control systems.

Information technology means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency.

Input controls refer to safeguards applied to the information entered into a computer or during the process of entering data into the computer.

Least Privilege is allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Library refers to the physical site where magnetic media, such as magnetic tape, is stored.

Medical information is protected health information that can be associated with an individual. Service providers supporting the ARC Program who have access to medical information are responsible for managing and handling medical information in compliance with Health Insurance Portability and Accountability Act (HIPAA) regulations. These Federal regulations are designed to protect the privacy of individuals requiring medical attention while allowing sharing of health information to promote public health.

Password is a sequence of characters that is used for authentication purposes to verify the identity of an authorized user and to grant the user access to a computer system. *Personnel screening* refers to the process of investigating the background of candidates to determine their suitability for a given position. For example, in positions with high-level fiduciary responsibility, the screening process will attempt to ascertain the person's trustworthiness and appropriateness for a particular position.

Personally Identifiable Information (PII) is any information about an individual maintained by an agency, including: (i) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (ii) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Organizations' definitions of PII may vary based on the consideration of additional regulatory requirements.

Physical access control refers to the type of control that involves restricting physical access to computer resources and protecting these resources from intentional or unintentional loss or impairment.

Program review is an overall information security program review, which is required annually.

Purging is a media sanitization method that is more extensive than clearing which can be achieved for magnetic media by degaussing, which destroys the media on which the data is stored. In order to purge data from non-magnetic media, the media must be destroyed, which can be accomplished by disintegration, incineration, pulverizing, shredding, or melting.

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk.

Security awareness includes materials such as presentations, posters, banners, newsletters, and activities such as security awareness days that are used to focus attention on information security concerns and appropriate responses to information security incidents.

Sensitive Information (SI) refers to information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use could adversely affect the ability of an ARC Program to accomplish its mission, proprietary information, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act.

Segregation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process.

Service Accounts are any accounts used by vendors or maintenance personnel for administering/servicing the systems.

System Owner is the individual responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.[9]

System Manager is the individual(s) who has the operational responsibility for following operational procedures supporting the procurement, development, integration, modification, or operation and maintenance of an information system.

Threats are activities, deliberate or unintentional, with the potential for causing harm to an automated information system or activity.

Users are people or processes accessing an IT resource either by direct or indirect connections.

Virus is a program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.

Vulnerabilities are flaws or weaknesses that may allow harm to occur to an automated information system or activity.

[9] The responsibilities of the system owner and manager are different than the responsibilities of the owner and manager of the information that resides on the system. The types of systems supporting the mission of the ARC Program are listed in the *ARC Program Information Systems* section provided earlier in this document.

Appendix B: References

Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.

Freedom of Information Act, 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996.

Health Insurance Portability and Accountability Act (P.L. 104-191), August 1996.

Public Law 93-579, The Privacy Act of 1974, as amended.

Public Law 99-474, Computer Fraud & Abuse Act of 1986.

Public Law 100-235, Computer Security Act of 1987.

Public Law 104-13, Paperwork Reduction Act of 1978, as amended in 1995, U.S. Code 44 Chapter 35.

Public Law 104-106, Clinger-Cohen Act of 1996 (formerly known as the Information Technology Management Reform Act).

Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Transmittal 4, November 28, 2000.

Appendix III to OMB Circular A-130, *Security of Federal Automated Information Resources*, November 28, 2000.

Office of Management and Budget Memorandum M-06-16, *Protection of Sensitive Information*, June 2006.

National Institute of Standards and Technology Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, May 2001.

National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

National Institute of Standards and Technology Special Publication 800-39 (Second Public Draft), *Managing Risk from Information Systems: An Organizational Perspective*, April 2008.

National Institute of Standards and Technology Special Publication 800-53 Rev 3 (Errata as of May 1, 2010), *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

National Institute of Standards and Technology Special Publication 800-53 Rev 3, *Appendix J, DRAFT Privacy Control Catalog,* July 19, 2011.

National Institute of Standards and Technology Special Publication 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Updated with Errata page May 7, 2013).

National Institute of Standards and Technology Special Publication 800-60, Revision 1, *Guide for*

Mapping Types of Information and Information Systems to Security Categories, August 2008.

National Institute of Standards and Technology Special Publication 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, October 2008.

National Institute of Standards and Technology Special Publication 800-66, Revision 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, October 2008.

National Institute of Standards and Technology Special Publication 800-88, *Guidelines for Media Sanitization*, September 2006.

National Institute of Standards and Technology Special Publication 800-122 (Draft), *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, January 2009.

National Science Foundation, *Information Security Handbook, Manual* 7, Office of Information & Resource Management, Division of Information Systems, July 9, 2013.

National Science Foundation *Manual 14, Personnel Manual* Office of Information and Resources Management, May 21, 2010.

National Science Foundation Bulletin 08-09, NSF Policy on Reporting the Breach of Personally Identifiable Information, May 1, 2008.

National Science Foundation, Computer Security Incident Response Plan Version 2.0, Office of Information & Resource Management, Division of Information Systems, April 28, 2014.

Appendix C: Arctic Incident Response & Reporting

The ARC Incident Response Plan addresses incident identification, handling, response, and notification policy and procedure for ARC program IT&C service providers, contractors, grantees, and teaming partners governed by cooperative agreement. The plan expands upon the policy provided in this handbook to address specific procedures for all staff who support the ARC program and provides relevant templates and contract information to adequately conduct Incident Response in accordance with this policy and includes guidelines for evidence handling as well as incident reporting. The ARC Incident Response Plan is included in its entirety and begins on the next page of this appendix.

National Science Foundation
Division of Polar Programs
Arctic Sciences Section
Research Support and Logistics

IT Incident Response Plan

Version 0.8

For Official Use Only

1. Introduction

The Information Technology (IT) Incident Response (IR) Plan is customized to meet the unique needs and requirements of ARC Research Support and Logistics (RSL) so that incident response is performed effectively, efficiently, and consistently. This plan also provides guidance for IR team interactions with other teams within the ARC Program.

This document is aligned to incident response policies provided in the *NSF PLR Arctic Sciences Section Information Security Handbook*, *NSF Office of Information and Resource Management Division of Information Systems, Computer Security Incident Response Plan*, and is based on Federal guidance provided by NIST SP 800-61 Rev 2, *Computer Security Incident Handling Guide*, and NIST SP 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

The ARC Incident Response Plan is a component of the ARC Information Security Program which is designed to ensure adequate security measures are in place to address security considerations directly related to ARC Program mission and supporting business processes. As stated in the Arctic RSL Program Synopsis available on the NSF website:

> *The Arctic Research Support and Logistics (RSL) Program supports the fieldwork of research projects funded through science programs in the Arctic Sciences Section … and in some cases proposals funded elsewhere at NSF and at other agencies. The RSL program also supports facilities and services to the research community through grants, cooperative agreements and contracts to organizations. The RSL program invests in some research and development activities to improve efficiency, safety and access to the Arctic.*

1.1. Audience Distribution and Revision Cycle

This IR Plan may be distributed program-wide as part of the Information Security Handbook but provides detailed instruction only for those personnel who may be involved in responding to an information security incident that impacts or involves the ARC Program. General ARC Program personnel and participants including the research community will receive separate guidance independent of this plan through general information security awareness training on expectations for escalating a suspected security incident to the incident response team, and on their role in supporting incident response.

This plan is reviewed on an annual basis, and if necessary is revised to address system/organizational changes or problems encountered during plan implementation or execution. When revisions are made the IR plan is redistributed. To protect the IR Plan from unauthorized disclosure, this document should be securely stored and distributors should utilize secure mechanisms for transmission.

1.2. Purpose

ARC IT and Communications (IT&C) service providers collaborate with the ARC Information Security Team and ARC RSL Program Managers (PMs) to establish processes and tools that effectively identify and detect incidents, evaluate the threat, report incident specifics appropriately, implement corrective action, capture lessons learned, and close out the incident.

The IR Plan tailored for the ARC-program addresses:

- Defining the categories of reportable incidents and the time period in which suspected incidents are to be escalated or notified to those identified as responsible for providing guidance on and for managing the incident
- Developing and disseminating procedures for performing incident handling and reporting,

based on the IR policy and IR Plan

- Selecting a team structure and staffing model for responding to potential incidents
- Determining what services the incident response team should provide
- Setting guidelines for communicating with service providers or outside parties regarding incidents
- Training potential incident response team members
- Coordinating incident handling and contingency planning activities
- Incorporating lessons learned from ongoing incident handling activities into incident response procedures and training

1.3. IT Events and Security Incidents

An IT event is any observable occurrence in a system or network such as a user connecting to a file share, a server receiving a request for a web page, a user sending email, or a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.

This IR Plan only addresses adverse computer security-related events, not those caused by natural disasters, power failures, etc.

A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of incidents include the presence of viruses or other malicious software; network probes, attacks or penetration; denial of service, the assumption of control of an information resource by an unknown or unauthorized user, or the breach of sensitive or Personally Identifiable Information (PII).

For the ARC Program, any activity that is a threat to the confidentiality, integrity, or availability of information resources, has the potential to undermine science or operational activities, presents legal issues related to sensitive data, or the misuse of government information resources may be an information security incident.

1.4. Process and Guidance Structure

Figure 1 depicts the guidance, policies, processes, and procedures that facilitate incident response at different levels across the ARC Program, and within the overarching Federal and NSF Agency requirements.

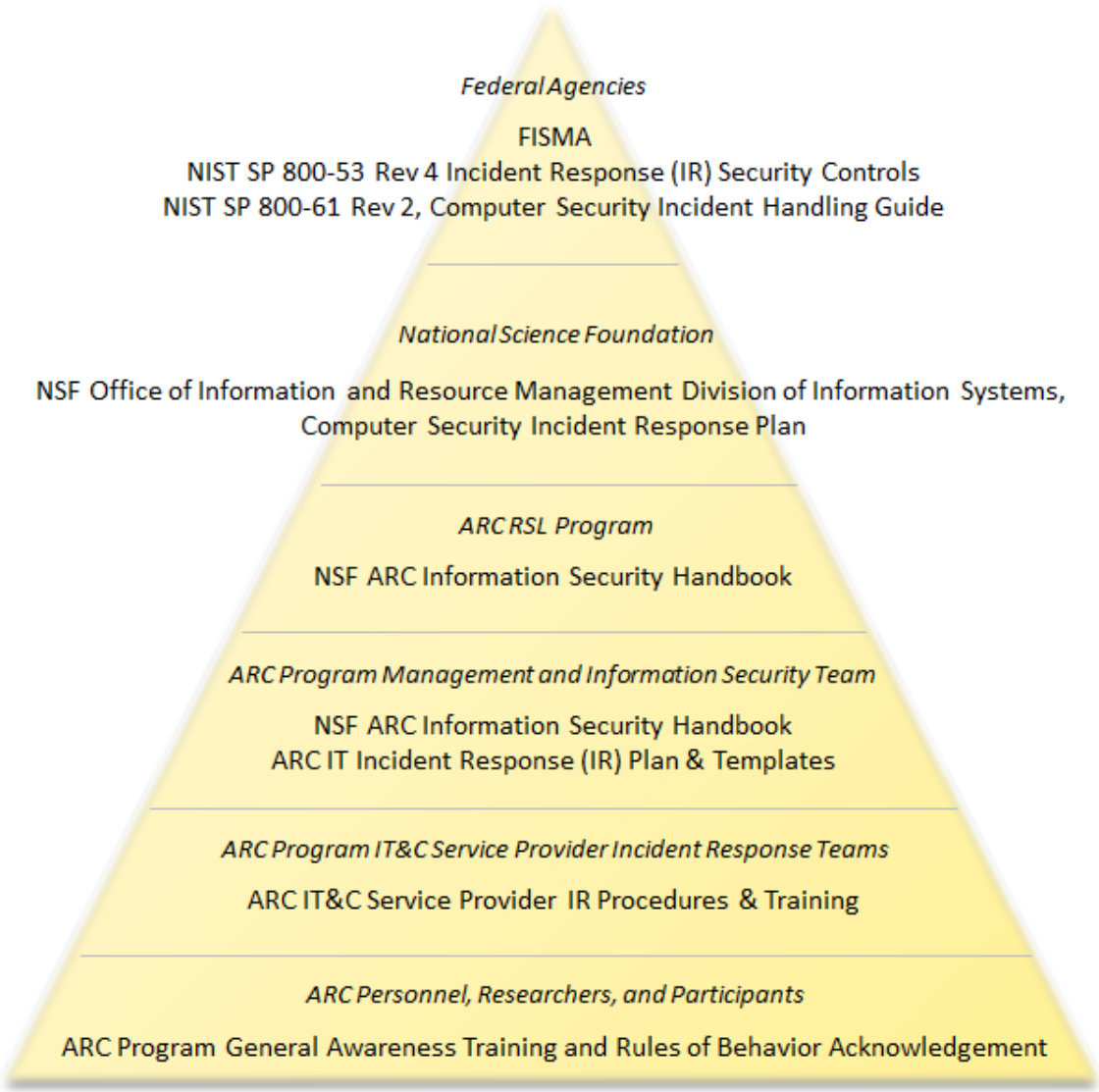

Figure 3. NSF PLR ARC Incident Response Documentation Structure

2. Guidance for IT&C Service Providers

This section provides guidance that should be referenced by all ARC IT service providers for implementing incident response capabilities. Incident response procedures should be developed to address preparation, detection and analysis, containment, eradication and recovery, and post-incident activity.

ARC IT service providers are responsible for implementing NIST compliant incident response procedures that address the requirements of this ARC RSL IR Plan, ARC Information Security Handbook Incident Response policy, and all aspects of incident response as defined by NIST SP 800-61 Rev 2, *Computer Security Incident Handling Guide*, and NIST SP 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

ARC IT service providers are also responsible for ensuring IR Team members are adequately trained on ARC IR procedures before responding to an incident, and receive annual refresher training thereafter.

2.1. Preparation

To prepare for handling an information security or computer security incident, IT service providers should establish internal IR procedures, identify potential IR team members, and identify systems, services, and data that may serve as a resource in detecting, analyzing, containing, eradicating, recovering from, or reporting on an incident.

Useful tools and resources for handling an incident include multiple communication and coordination methods, current contact information for potential IR team members and those who may be contacted when escalating or reporting an incident, incident documentation templates included a chain of custody log, secure storage for proper handling of evidence, issue tracking system/process for maintaining a record of activities as IR progresses, and a FIPS-compliant encryption method for securely sharing incident related data among IR team members and for escalating and reporting purposes.

2.2. Detection and Analysis

Upon detection or notification of a suspected information security incident, the first step is to confirm if an actual incident is in progress or has occurred.

Incident responders determine if an event is actually an incident through analyzing symptoms that are often ambiguous, contradictory, and incomplete. At times it may be necessary for different roles to collaborate to make the decision on if an incident is in progress, has transpired, or should be escalated and/or reported. Throughout the incident response process there is a delicate balance of limiting disclosure of incident-related information and engaging those required to respond. Incident responders should always limit dissemination of information regarding the incident to only those with an operational 'need to know' regardless of their rank or position within the organization. At times this may mean for example that those involved in the detection and analysis step may not be privy to details on the complete resolution and closure of the incident.

When the IR team believes an incident may have occurred or is in progress, the team should follow a pre-defined process and document each step taken while determining the scope, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring (what attack methods are being used, what vulnerabilities are being exploited). Specifically when there is even a suspicion that PII may have been breached the potential for disclosure must be immediately reported.

Initial analysis of a suspected incident serves as the foundation for the technical IR team to work with the IR Manager and ARC Information Security Team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident.

2.3. Document Activities

Templates for creating documentation in support of computer security incident response are provided as attachments to this IR Plan. Every step taken from the time the incident was detected to its final resolution should be documented and time stamped. Every document regarding the incident should be dated and signed by the incident handler. Information of this nature can also be used as evidence in a court of law if legal prosecution is pursued. Whenever possible, handlers should work in teams of at least two: one person can record and log events while the other person performs the technical tasks.

IR documentation should include the current status and summary of the incident, incident indicators and references to other potentially related incidents, actions taken by all incident handlers on this incident, chain of custody, if applicable impact assessments related to the incident, contact information for other involved parties, a list of evidence gathered during the incident investigation, comments from

incident handlers, and proposed next steps to be taken.

The IR team should safeguard incident data and restrict access to it because it often contains sensitive information. Incident-related communications and documents should be encrypted or otherwise protected so that only authorized personnel can read them.

2.4. Prioritize Incident Handling

Use the following guidelines to determine the priority responding to an incident should take in relation to other operational activities. A combination of these factors should be considered for prioritizing IR activities. The team should prioritize the response to each incident based on its estimate of the business impact caused by the incident and the estimated efforts required to recover from the incident.

Functional Impact *The resulting negative impact to system users/ system functionality including the current impact of the incident and the potential longer term impact if the incident is not immediately contained and eradicated.*	
High	Some critical services are not available to any users
Medium	A critical service is not available to a subset of system users
Low	Critical services are available to all users but may have lost efficiency
None	No effect to the ability to provide all services to all users
Information Impact *How potential effects of the incident to the confidentiality, integrity, and availability of ARC Program information may impact the overall mission.*	
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or transferred without authorization
Integrity Loss	Sensitive or proprietary information was changed or deleted
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or transferred without authorization
None	No information was accessed or transferred without authorization, changed, deleted, or otherwise compromised
Recoverability Effort *The amount of time and resources it will take to recover from an incident. This measure is typically based on the size of the incident and the type of resources it affects. The recoverability effort should be focused on addressing the specific losses incurred from the incident, followed by process improvements to ensure a similar incident does not occur in the future.*	
Not Recoverable	Recovery from the incident is not possible (e.g., unauthorized transfer of sensitive data and posted publicly); launch investigation
Extended	Time to recovery is unpredictable; additional resources and outside help are needed

Supplemented	Time to recovery is predictable with additional resources
Regular	Time to recovery is predictable with existing resources

2.5. Notification, Escalation and Reporting

When an incident is analyzed and prioritized, the incident response team needs to notify the appropriate individuals so that all who need to be involved will play their roles. This section provides ARC IR teams with requirements for what must be reported to whom and at what times.

CH2M HILL Polar Service (CPS) manages various IT&C resources for the NSF ARC Program, as provided for by the Arctic Research Support and Logistics Services contract with CH2M HILL Constructors, Inc. (CCI). CPS is composed of personnel from CCI, Polar Field Services (PFS), SRI International, and Ukpeaġvik Iñupiat Corporation (UIC). Additional IT&C resources are managed by other partner entities. Appropriate notification points of contact for incident response are identified in the table below and further defined in section 2.5.3 Notification Call Tree.

Field Site/IT Asset Type	Notification for Incident Response
Barrow, AK Field Station	CPS
Fairbanks, AK Field Station	CPS
UAF Operated IT&C at Toolik Field Station	Follow UAF Protocol
Toolik Field Station SCADA Data, Industrial Control Systems, Iridium Phones, IT Satellite or remote field stations	CPS
Greenland Field Stations (non-military personnel)	CPS
Military Support Program-wide	Follow branch protocol (ANG, Navy, etc.)

Suspected and confirmed information security incidents are tracked and documented by ARC IT&C service providers. ARC IT&C service providers use the *ARC Information Security Incident Reporting* Template to report technical incidents and potential PII disclosure incidents that occur on IT&C systems and services supporting the ARC program. Reporting incidents in a timely manner is critical. ARC IT&C service providers are to engage the ARC Information Security Team as soon as possible when investigating a confirmed incident, and report details of the incident as soon as possible to ARC RSL PMs. Incident reports are iteratively updated as more information about the incident is discovered through the incident handling process.

For incidents reported to ARC RSL PMs, internal NSF policies and procedures are followed to determine if further escalation of the incident is required. In these cases RSL PMs refer to the *NSF Office of Information and Resource Management Division of Information Systems, Computer Security Incident Response Plan* for guidance.

For all reportable incidents the IT&C service provider should deliver initial notification following detection, analysis, and prioritization of the incident, provide regular updates and draft reports as incident resolution progresses, and a final report upon closure of the incident.

2.5.1. Reportable Security Incidents

The following types of incidents must be reported as outlined in the *Incident Escalation Matrix*.

- Privacy breach - Sensitive personally identifiable information (PII) was accessed or transferred without authorization
- Proprietary breach - Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or transferred without authorization
- Integrity loss - Sensitive or proprietary information was changed or deleted
- Unauthorized access to systems or data
- Denial of Service (DOS)
- Malware, Trojan, virus infection spread to multiple systems
- Physical breach or damage
- Copyright infringement
- Illegal activity
- Unauthorized monitoring of network activity

2.5.2. Incident Escalation Matrix

Suspected and confirmed information security incidents must be reported to designated roles within the designated timeframes outlined below.

For those incidents marked for notification of detection within one hour of suspected incident, individuals who discover the incident should make appropriate contact as determined by their governing organization and ARC InfoSec team members immediately for help troubleshooting the problem. They will provide confirmation of an "incident" as defined by this plan and provide guidance for further notification or take on the action of notification to the RSL PMs themselves.

For all other notification timeframes, notification to appropriate organizational contact and ARC InfoSec team should take place within the earliest possible timeframe, with the goal of providing sufficient time for the InfoSec team to notify the RSL PMs within the timeline identified in this document.

Incident Type	Notification Timeframe	Role(s) to Notify
Privacy Breach	1 hour from detection of suspected incident	**CPS Groups Notify:** CPS Head of IT, ARC InfoSec Team Members, & RSL PMs **UAF Operated IT at TFS:** Follow UAF Protocol **Military Program**
Proprietary Breach	1 hour from detection of suspected incident	
Integrity Loss	1 hour from detection of suspected incident	
Unauthorized Access	1 hour from confirmation of the incident	
Denial of Service	1 hour from confirmation of the incident	
Virus Spread	1 day from confirmation of the incident	
Physical Breach/Damage	1 day from confirmation of the incident	

Copyright Infringement	1 day from confirmation of the incident	**Support**: Follow branch protocol (Airforce, Coast Guard, etc.)
Illegal Activity	1 hour from confirmation of the incident	
Unauthorized Monitoring	1 day from confirmation of the incident	

2.5.3. Incident Notification Call Tree

Refer to the following contact information for notifying and escalating a reportable incident. As stated above in 2.5, various entities mange various IT resources.

Managing Organization	**Name/Role**	**Contact Information**	**Notification Escalation Protocol**
CH2M HILL Polar Services	Michael Lilly CH2M HILL Polar Services Head of IT	720-286-4326 Mobile: 719-321-1544 Michael.Lilly@ch2m.com	Notify Michael Lilly immediately upon discovery of a suspected or confirmed incident.
	Mike McKibben CH2M HILL Polar Services Program Manager	720-286- 0410 Mobile: 303-885-4644 mike.mckibben@ch2m.com	If Michael Lilly is unreachable after 3 attempts or 15 minutes, contact Mike McKibben.
	David Smith CH2M HILL Polar Services Assistant Program Manager	720-286-3219 David.Smith3@ch2m.com	If Mike McKibben is unreachable after 2 attempts or 10 minutes, contact David Smith. The CPS contact will aid in determination of incident and provide direction on further escalation to other staff listed in this call tree.
	If none of the CPS contacts can be reached, proceed to notify a member of the ARC Information Security Team, below.		
Military Support Program-wide	Follow your respective branch protocol, then proceed to notify a member of the ARC Information Security Team, below:		
UAF IT	UAF operated/responsible IT at TFS		Follow UAF procedures and escalation protocol, then proceed to notify a member of the ARC Information Security Team, below:

Managing Organization	Name/Role	Contact Information	Notification Escalation Protocol
Any Organization as advised above	Maria Petrie/ ARC Information Security Team	843-743-7512 Mobile: 706-414-1412 petrie_maria@bah.com	Engage at least one ARC Information Security Team member following the initial analysis phase. Maria, Petrie, Sarah Vasel. The ARC Security Team will contact and notify a member of the ARC RSL PM Support Team.
	Sarah Vasel/ ARC Information Security Team	843-364-3350 vasel_sarah@bah.com	
	Gary Eells/ ARC RSL Program Management Support	571-512-2538 geells@associates.nsf.gov	ARC Information Security Team will notifiy ARC RSL PM Support to provide situational awareness and status updates as confirmed incidents are in the process of being addressed.
	Randy Olsen/ ARC RSL Program Management Support	571- 512-2540 rolsen@associates.nsf.gov	
	Patrick Haggerty/ ARC RSL Program Manager	703- 292-8577 Mobile: 703-338-4762 phaggerty@nsf.gov	The ARC Security Team will notify a member of the ARC RSL PM Support Team upon confirmation that an incident had a negative impact to system users/ system functionality or resulted in a data breach.
	Renee Crain/ ARC RSL Program Manager	703-292-4482 Mobile: 703-589-8990 rcrain@nsf.gov	

2.6. Choose a Containment Strategy

Containment of an incident in progress ensures other systems and resources remain unaffected by the incident, and allows for further analysis before a remediation/eradication solution is selected and executed. Criteria for determining the appropriate containment strategy include:

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability to users once the containment strategy is in place
- Time and resources needed to implement containment
- Effectiveness of the strategy in containing the impacts of the incident

- Duration of the solution for complete eradication and recovery from the incident

2.7. Evidence Gathering, Handling and Retention

While evidence is primarily gathered to resolve an incident, it may also be required for legal proceedings following an incident. To prepare for this potential outcome it is important to clearly document how all evidence, including compromised systems, has been preserved. It is also beneficial to review evidence collection procedures with legal staff to ensure the process meets all applicable laws and regulations are addressed so that any evidence can be admissible in court.

Evidence should be accounted for at all times; whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature. A detailed log including the following details should be kept for all evidence:

- System identification (location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer)
- Name, title, and phone number of each individual who collected or handled the evidence during the investigation
- Time and date (including time zone) of each occurrence of evidence handling
- Locations where the evidence is/was stored

When collecting evidence remember that it is much better to capture a snapshot of the system as-is rather than doing so after incident handlers, system administrators, and others have inadvertently altered the state of the machine during the investigation. Users and system administrators should be made aware of the steps that they should take to preserve evidence during and following an incident.

Following resolution of an incident, evidence should be retained and securely stored until ARC RSL PMs approve sanitization of systems and data storage devices.

2.8. Eradication and Recovery

To complete eradication and recovery following the containment of an incident, restore systems to operation and confirm systems are functioning normally. If applicable, remediate vulnerabilities on other systems to prevent similar incidents. Addressing other similar vulnerabilities in the environment or in the organization following an incident is critical to lowering the likelihood of a similar incident occurring again, as once a resource is successfully attacked, it is often attacked again, or other resources within the organization are attacked in a similar manner.

Depending on the severity of the incident, an IT Contingency Plan and supporting procedures may be referenced to perform system recovery and restoration. In cases where CP procedures are followed, recommended improvements to procedures should be notated while recovering the system, and reviewed as part of lessons learned.

Recovery may include an increase in information security awareness and training to inform ARC personnel and participants of potential incidents that they may be a target for. Human interaction is often required for an exploit or breach to be successful, making awareness communications a critical part of the incident recovery strategy.

2.9. Lessons Learned

Following each noteworthy incident, the IR team should hold a lessons learned meeting with all involved parties to identify ways to improve security measures and the incident handling process itself.

If appropriate, multiple incidents can be covered in a single lessons learned meeting, however the meeting should be held shortly after an incident is closed to avoid loss of information and feedback as time passes. Lessons learned meeting results should be captured in the *ARC RSL Incident Response Lessons Learned* template attached to this IR Plan.

Lessons learned results and identified process improvements should also be implemented in the applicable IT Contingency Plan and supporting procedures to address potential weaknesses identified as an outcome of the incident.

2.10. Training

The ARC Information Security Team in partnership with ARC IT&C service providers facilitates incident response training for personnel who may be involved in responding to a suspected incident consistent with assigned roles and responsibilities. Training is provided when an individual or group assumes an incident response role or responsibility, and on an annual basis thereafter.

ARC Program operational personnel and participants, including the research community will receive explicit guidance as part of general information security awareness training on how to notify proper personnel in the case of a suspected incident and expectations for their support during the incident response process.

2.11. Testing

As required for a moderate system, the ARC IR Team should perform testing of the incident response capability for the ARSLS Program Application System on an annual basis to determine the incident response effectiveness and document the results. Incident response testing may include the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises to determine the potential effects an incident could have on ARC Program operations. If appropriate, IR procedures may be tested as part of an IT contingency plan test scenario.

3. Templates

ARC IR Teams should use templates provided in this section for IR reporting and lessons learned. Final IR reports and lessons learned documents should be delivered to ARC RSL PMs for oversight and record management purposes.

3.1. ARC RSL Incident Response Report

ARC IR reporting template 17July2014.

3.2. ARC RSL Incident Response Lessons Learned

ARC Incident Lessons Learned Ter

3.3. ARC RSL Chain of Custody Log Template

IR Chain of Custody Log Final.docx

Appendix D: ARC VRAT Management Process

The Arctic program VRAT serves to facilitate management processes that identify security weaknesses in the ARC program and outlines recommendations and milestones necessary for mitigation. All process information, record storage information, and details on the ARC Risk Management policy are fully defined in the ARC VRAT Management Process. The ARC VRAT Management Plan is included in its entirety and begins on the next page of this appendix.

National Science Foundation

Division of Polar Programs

Arctic Sciences Section

Vulnerability Remediation Action Tracker (VRAT) Management Process

Version 0.4

Overview

The Arctic program Vulnerability Remediation Action Tracker (VRAT) serves to facilitate management processes that identify security weaknesses in the ARC program and outlines recommendations and milestones necessary for mitigation. This ARC VRAT Management Process will be used to formalize and facilitate the remediation of ARC program- and system-level weaknesses, and will provide a means for:

- Planning and monitoring corrective actions;
- Defining roles and responsibilities for weakness resolution;
- Assist in identifying funding requirements necessary to mitigate weaknesses;
- Tracking and prioritizing resources;
- Informing Arctic Program Research Science and Logistics (RSL) Program Managers (PMs); and
- Ensuring decision makers have a regularly scheduled opportunity to review VRAT items.

VRAT Purpose

The VRAT and its supporting processes enhance the NSF RSL PM's ability to identify, assess, prioritize, and monitor progress of corrective actions pertaining to information security weaknesses found within sites and systems managed by the ARC program. This VRAT management process will instruct stakeholders in their role in VRAT management, but will not be a comprehensive plan for closing individual VRAT items. More detailed project management plans may be created as needed for each corrective action item identified in the VRAT, based on original source documents in which weaknesses were first identified (e.g. Risk Assessments, Security Control Assessments, Continuous Monitoring activities, etc.).

VRAT Management Tools

The following tools are used for capture, tracking and reporting of ARC Program VRAT items. These tools are managed by the ARC security team. To ensure configuration control and traceability, only the ARC Security team and Michael Lilly, CPS head of IT, have access and can make updates to the Microsoft PowerPoint VRAT slide decks.

- GSS VRAT Slide Deck
- ARSLS VRAT Slide Deck
- Microsoft Excel VRAT Master List (internal ARC security team management document)

Tools are stored and updated on an internal ARC security team SharePoint site:
https://pmev2.bah.com/ecs/FC_FederalC-A/nsfarctic/VRATsite/default.aspx

VRAT Review Plan & Schedule

Effective use of the VRAT requires a regular review cycle including three critical functions: review of open items, resource planning for mitigation, and validation of completion. This VRAT Management Plan establishes a schedule for those activities and provides Arctic program processes to complete these activities. Normalizing VRAT Management procedures as routine program support is critical to

maturation of the ARC Information Security Program and the ability of NSF to sustain secure IT resources for awardees.

The following activities will occur as part of the VRAT review cycle.

Ongoing:

- **Discovery & VRAT Creation**– Weaknesses are discovered through ongoing ARC Security program Continuous Monitoring activities such as: Vulnerability Assessments/Scans, Security Control Assessments, Risk Assessments, etc.
    1. Weaknesses are first reviewed and verified with the responsible stakeholder.
    2. Confirmed weaknesses will be incorporated into the VRAT process deck for easy reference and follow up, which includes:
        - Assignment of a VRAT #
        - Detailing the vulnerability, risk, proposed solution, steps to completion/ milestones and draft schedule
- **VRAT Prioritization and Scheduling-** Since introduction of new VRAT items is ongoing, prioritization activities serve to ensure the right VRATs are being addressed first (e.g., more critical weaknesses, low LOE/high impact mitigations, etc.). These scheduling and prioritization discussions will occur regularly between CPS and the ARC Security team.

Monthly:

- **Data Call/Update –** ARC security team will email request to CPS and IT stakeholders for verbal or emailed updates to their respective VRAT Items. ARC security team will update the VRAT slides.

Quarterly:

- **ARC IT Stakeholder VRAT Update** – On a quarterly basis, stakeholders with assigned VRAT items are responsible for providing updates to their respective VRAT items, and reporting progress on assigned milestones
    - CPS stakeholders report updates to CPS Head of IT (currently Michael Lilly)
    - CPS head of IT is responsible for consolidating CPS input and updating the VRAT slides on ARC security team SharePoint site: https://pmev2.bah.com/ecs/FC_FederalC-A/nsfarctic/VRATsite/default.aspx
    - All other IT stakeholders report updates to ARC Security Team
    - ARC security team validates IT stakeholder update/milestone actions and formally closes out VRAT items that have been addressed
    - ARC security team reviews the VRAT item in general to determine if the weakness is current, milestones are accurate and up to date, and if the VRAT should be consolidated or grouped with a similar existing VRAT item.
- **VRAT Update /Resource Planning Meeting -** Once quarterly updates from IT Stakeholders are consolidated, the ARC security team will meet with oversight support from ALEX (currently Gary Eells) to provide update and discuss resource planning.
- **RSL PM VRAT Status Update**– Quarterly update will be shared by ARC security team to RSL PMs. The ARC Information Security Team will advise RSL PMs of VRAT items completed, nearing completion, in danger of missing milestones, or those requiring updated

resource/funding decision. RSL PMs determine next steps for VRATs, which include;

- VRAT closure via Acceptance of Risk
- VRAT approved for additional resources to support execution
- VRAT approval for mitigation with existing resources

- **IAWG Meeting-** Review non-sensitive VRAT updates/closures, gather feedback and discuss impacts

Annual VRAT Management Plan Schedule

Continuous/Ongoing Activities **Discovery & VRAT Creation**– Weaknesses are discovered through ongoing ARC Security program Continuous Monitoring activities **VRAT Prioritization and Scheduling-** Since introduction of new VRAT items is ongoing, quarterly scheduling activities serve to ensure the right VRATs are being addressed first (e.g., more critical weaknesses, low LOE/high impact mitigations, etc.)		
Date/Frequency	**Activity**	**Assignments (Roles)**
Monthly 2nd week of each month	**Monthly VRAT Data Call** – Email IT stakeholders to for any updates on open VRAT items	ARC Security Team (facilitator) CPS (contributors) Other ARC IT Stakeholders (UAF, TFS, etc.)
Quarterly January April August October	**ARC IT Stakeholder VRAT Update –** Formal full update of VRAT Tools (slides, spreadsheet)**,** review and update of all milestones and validation of VRAT closures.	ARC Security Team (facilitator) Other ARC IT Stakeholders (contributors) CPS (contributors)
Quarterly 2-3 weeks in advance of RSL PM Management meeting	**VRAT Update /Resource Planning Meeting –**present updates to ALEX for resource planning discussion	ARC Security Team (facilitator) ALEX (contributors)
Quarterly February May September December	**RSL PM VRAT Status Update** – Update RSL PM on VRAT items closed to date and progress on open VRAT items, including potential issues that could prevent remediation as schedule during the ARC Security Quarterly Management Meeting New VRAT items discovered in the reporting period will be shared as well.	RSL PMs (oversight/contributors) ARC Security Team (facilitator) ALEX (oversight support)
Quarterly January April September November	**IAWG Meeting** – Review Non-sensitive VRAT updates, gather feedback, discuss impacts. (IR Policy, HW/SW Maintenance Policy, etc.) ARC security team to capture any issues anticipated by IT stakeholders	ARC Security Team (facilitator) All IAWG Members (contributors)

Requirements to Close a Finding

For most VRAT items, the mitigation plan developed in collaboration with the IT service provider at the time the weakness was discovered will be implemented according to schedule and the item will be closed. Once VRAT items are fully mitigated, the ARC Security team will validate that the milestones have been completed. Once all remediation actions are completed and verified, the VRAT will be reported to RSL PM as "closed" and will be archived by the ARC Information Security team.

Acceptance of Risk (AOR)

In the event a vulnerability cannot be fully resolved, RSL PM may opt to close the VRAT item under the category "Acceptance of Risk." Acceptance of Risk is an acknowledgement of the vulnerability wherein the likelihood of exploitation has been weighed against the resources required for remediation and the determination is made that the vulnerability cannot be corrected within the means of existing program resources, or that the resources would be ill spent on the proposed corrective action. Though Acceptance of Risk acknowledges the problem cannot be completely fixed under present circumstances, due diligence still requires some mitigation of the vulnerability to reduce the risk presented to the enterprise. Acceptance of Risk for Medium or High risk vulnerabilities is generally inappropriate, and all efforts should be made to reduce the risk to Low before closing the VRAT item. Low risk findings may be closed via Acceptance of Risk at RSL PM discretion. Any VRAT item closed via Acceptance of Risk should be recorded on the ARC VRAT Acceptance of Risk Template.

ARC AOR Template v3.doc

AOR Maintenance

AORs can be approved by RSL PM's via email, or preferably via digital or written signature. For ease of reference, AORs should be saved and stored with the following naming convention: AOR_VRAT Name_Number_Date

AORs will be archived on the ARC Security team SharePoint site, and a copy of all and a copy of all AORs, supporting documents if any, and email string with PM review questions and answers and final approval will be provided to the program managers and oversight support from ALEX (currently Gary Eells) for storage on NSF document management systems.

VRAT Management Process Maintenance and Update

This VRAT Management Process should be reviewed annually to determine its suitability for the ARC program as mission needs and program resources change. As the program matures, the quarterly review may increase to monthly, for example, or any other interval RSL PMs determine best serves the needs of the program. Similarly, a more automated process may be implemented in future years for vulnerability management. If automation or any other major management change occurs, this plan should be revised accordingly.