ATTACHMENT E:

System Security Plan

NOVA Research Company

Systems Security Policy and Practices

NOVA Research Company currently provides information technology systems services to the National Institutes of Health, Centers for Disease Control and Prevention, and Health Research and Services Administration, including Web site development, maintenance and host operations. Therefore, NOVA is familiar with and in compliance with DHHS Certification and Accreditation (C&A) documentation and procedures requirements.

NOVA facility physical security is described in the NOVA Rules of Conduct.

NOVA's procedures for protection, controlling, handling or accessing Government data and other Automated Information Systems (AIS) resources, along with procedures for destruction of source documents and other contract related waste materials are described in this document. Also described in this document are physical storage procedures to protect Government data and other AIS resources during performance of a project and discussion of limitations on employees concerning reproduction, transmission, or disclosure of data and project information. Additional information will be provided and/or expanded upon as needed.

Other documents specific to a system development or operation contract, such as Firewall Information Worksheet, Baseline System Information, Host Characterization Worksheet, and similar documents, can be provided on request when a specific system and its requirements are identified and defined.

In addition, all NOVA IT staff annually complete both the NIH Information Security Awareness Course and the CDC Information Security Awareness Training. NOVA employees working with NIH and/or CDC systems of records have also read and completed Non-Disclosure Agreements. Additional information on personnel security practices and procedures, including procedures for new and departing staff are provided in the attached documentation.

Included documentation relating to NOVA's Systems Security Policy and Practices are:

- Data Collection Questionnaire For Certification Review. Additional details will be completed when specifics of projects requiring C&A are identified.
- NOVA Rules of Conduct Policy and Procedures.
- NOVA Incident Response Policy and Procedures.

May 25, 2008

Data Collection
For Certification Review

Major Application and General Support System
Overview Questionnaire

Sensitive – For Official Use Only

Table of Contents

1.0 SYSTEM IDENTIFICATION AND OVERVIEW

1.1 Name & Unique Identifier

TO BE COMPLETED WHEN IDENTIFIED

1.2 Organization Responsible for the System

TO BE COMPLETED WHEN IDENTIFIED

1.3 Information Contact(s)

	Business Steward	Business Steward	Security Steward
Name			
Title			
Address			
Phone			
Email			

1.4 Operational Status

TO BE COMPLETED WHEN IDENTIFIED

1.5 Major Asset and Critical Infrastructure Status

TO BE COMPLETED WHEN IDENTIFIED

1.6 Mission

TO BE COMPLETED WHEN IDENTIFIED

1.7 System Environment

TO BE COMPLETED WHEN IDENTIFIED

1.8 System Data

TO BE COMPLETED WHEN IDENTIFIED

1.9 System Users

User Category	Access Level (Read / Write)	Number (Est.)	Home Organization	Geographic Location

1.10 System Interconnection / Information Sharing

TO BE COMPLETED WHEN IDENTIFIED

1.11 System Dependencies

TO BE COMPLETED WHEN IDENTIFIED

1.12 Supported Programs and Applications

TO BE COMPLETED WHEN IDENTIFIED

1.13 Applicable Laws or Regulations Affecting the System

TO BE COMPLETED WHEN IDENTIFIED

1.14 Security Policy:

NOVA Research Company has been performing information technology contracts since its founding in 1986 and has been *compliant with Level 3 AIS requirements* for more than a decade. In order to assist reviewers in evaluating NOVA's AIS control procedures, the following pages provide NOVA's AIS Plan in accordance with *AIS Handbook* requirements posted at http://irm.cit.nih.gov/policy/aissp.html.

1. General Safeguards	
Security officer (Level 2)	NOVA has designated Paul Young, Executive Vice President and senior information systems professional, as NOVA's Security Officer for physical and environmental security, computer systems security, personnel screening, and documents/documentation security. Mr. Young has over 25 years of experience with computer security in a variety of DoD and civilian agency environments; was a DoD personnel and document security specialist; and, in collaboration with NOVA's Chief Technology Officer and Director of Network and System Operations, developed and implemented NOVA's AIS Security Plan and Office Security Plan.
Security training (Level 1)	NOVA Research has an employee security awareness program in place and provides periodic training in security procedures. This training includes a thorough understanding of the measures detailed herein in the areas of premises, workstation, and network security as they pertain to the data sensitivity and integrity of both NOVA and its clients. All individuals assigned to this project will be given refresher training in office and computer security awareness.
Personnel screening including assignment of sensitivity designations (Level 1) and required background investigations for all employees and contracted personnel (Level 2)	NOVA's Security Officer has implemented a security review and certification program in accordance with the DHHS *Automated Information Systems Security Program Handbook* (AISSP), Release 2.0, in conjunction with previous DHHS contracts for NIH and CDC. NOVA's Security Officer assigns security level designations to all NOVA personnel positions based on their level of AIS access and need to know. NOVA's Security Officer conducts periodic security level designation reviews of all NOVA personnel positions. As part of NOVA's SOP, all personnel, including contractors working on site or with sensitive data, receive an appropriate background investigation.
Risk analysis, including detailed risk management program and a CSSP for systems processing sensitive information (Level 2)	NOVA's Chief Technology Officer and Director of Network and System Operations has developed and distributed to senior management a detailed risk management program. The risk management program identifies threats and vulnerabilities associated with operation and maintenance of NOVA's information technology systems. These assessed threats and vulnerabilities include both internal and external vectors of attack via both physical and electronic means. He has also developed and distributed to senior management a Computer Systems Security Plan—a superset of the standard CSSP specifically for sensitive systems, with additional procedures for access control, auditing, integrity verification, and intrusion detection mechanisms. NOVA's Security Officer and Chief Technology Officer and Director of Network and System Operations jointly conduct a periodic formal risk analysis, in accordance with the DHHS *Automated Information Systems Security Program Handbook* (AISSP), Release 2.0.
2. Technical Safeguards	
Passwords/log-in, including a list of authorized users (Level 2)	All NOVA computers operate under Windows NT/2000 or Macintosh OS X. These operating systems are configured to require a unique valid ID and password before granting any access to the workstation. Multiple levels of local user permissions are implemented, and access can be controlled on a file-by-file basis. All significant activities are logged to a central server for review and archiving. NOVA's computer Standard Operating Procedures require all passwords to meet length and complexity requirements and to be changed monthly—policies that are enforced by the operating systems. In addition to workstation security, additional authentication is required to access data maintained on NOVA's networked

	file servers. All user identifiers have associated profiles that indicate what functions they are authorized to perform and data they are permitted to access (read, write, add, delete, change). Passwords are never displayed on any systems, and NOVA's Standard Operating Procedures prohibit any written records of passwords. NOVA's operating systems do not allow retrieval of forgotten passwords, instead requiring manual password reinitialization by a Systems Administrator and immediate subsequent personalization by the user.
Limit on log-in attempts (Level 2)	All computers and network databases utilize Windows NT domain security procedures, which have been configured to allow only three attempts to log on to any system. The user is then locked out of the AIS or database for one hour unless specifically granted access by a Systems Administrator. This policy effectively prevents brute-force password attacks. All operating systems used on NOVA workstations are configured to automatically lock down the terminal if it is not used for a predetermined period of time, via password-protected "screen savers." All users are required by NOVA SOP to maintain these features active with a maximum idle time of 15 minutes.
Physical access rights lists/profiles (Level 2)	NOVA's SOP is that only Company Directors and above have unrestricted access to NOVA's facility. Admission after hours is only by access key, which is automatically recorded by the facility security company. A list of all access keys by number, by authorized individual, is maintained by the NOVA Security Officer. The NOVA network server is maintained in a locked room inside NOVA's locked facility with access restricted to Corporate Officers.
Electronic access rights lists/profiles (Level 2)	Every NOVA user initially defaults to no access to electronic data. Access rights are granted only on a need-to-know basis, with write/change permissions assigned only as necessary. Shared data and associated access rights are segregated by project, task, subtask, etc. to an appropriate level of granularity based on sensitivity of the data. Only Systems Administrators are permitted to log on to the server consoles, prohibiting ordinary users or intruders from accessing any control or configuration parameters in the event of a physical security breach. All machines are configured via password-protected BIOS settings to disable booting from any removable media, further protecting systems from any unauthorized tampering. Modification of these functions can be accomplished only by Systems Administrators. In the event of their absence in an emergency, NOVA's President holds the key to an offsite safe-deposit box containing a complete set of authorization codes for use by contingency personnel.
Audit trail mechanisms (Level 2)	All of the operating systems and network hardware in use at NOVA contain built-in audit trail mechanisms. The Windows NT domain server and ancillary servers store all log-on attempts and significant access events, flagging unusual activity with a warning symbol to clearly stand out from routine operation. All workstations, firewalls, switches, routers, etc. are similarly configured to report a level of detail balanced to enable reconstruction of an incident without generating overwhelming volume. Server and hardware logs are reviewed weekly, and workstation logs monthly, by a Systems Administrator, using software that filters and categorizes events into patterns that are conducive to interpretation. Logs are then archived and backed up to permanent media before being cleared.
Dial-back—optional (Level 2)	For remote dial-in users, a layer of security in addition to the operating system level is implemented, requiring the presence of a 128-bit encrypted key on the remote computer, which has been previously registered with the Shiva LanRover remote access server. This key is demanded during

	challenge-and-response authentication by the handshaking software. Failure to provide this key results in immediate disconnection. The Shiva LanRover can easily be configured to perform call-back verification—yet another authentication procedure. Additionally, the LanRover maintains a complete protected audit trail of all log-on information, including successful and failed log-ons, which can be easily reviewed for a pattern of break-in attempts.
Message authentication—optional (Level 2)	NOVA's Microsoft Exchange e-mail and messaging platform has the built-in capability for authentication in the form of digital signatures. These signatures consist of encrypted private and public key pairs, the former used to sign messages, and the latter used to verify the identity of the signer. This system can be used to perform both messaging encryption and authentication in tandem with compatible client systems. NOVA also has the capability to use the less-integrated but more widely supported Pretty Good Privacy (PGP) software that implements similar Public-Key Infrastructure (PKI) to accomplish the same functions.
Encryption—optional (Level 2)	NOVA is familiar with, and has used in the past, numerous encryption mechanisms, including PKZip password hashing, PGP private/public key pairs, file-system encryption built into Windows 2000 and Mac OS X, Secure Sockets Layer (SSL) Internet transactions, and various methods involved in securing Virtual Private Networks (VPN), such as MD5, SHA1, and Triple-DES encoding. This breadth of familiarity enables NOVA to quickly adopt and gain facility with the preferred encryption standards of its clients or recommend data encryption methodologies as appropriate.
3. Operational Safeguards	
Backups (Level 2)	NOVA maintains a robust data backup and recovery system. All servers are backed up daily, and workstations monthly, with tapes immediately rotated offsite after each cycle. Retired data are periodically archived to optical media, with a copy stored both on- and offsite. In a worst-case scenario in which all servers and workstations are destroyed, offsite backup tapes could be used to completely restore all systems. Server data would be at most 1 week old, and workstation data potentially 1 month old. All critical working files and shared databases are resident on the file server to provide optimum availability. In addition, each NOVA staff member has a data directory on the server for backing up current working data sets, be it an analysis, a report, or correspondence. Using Computer Associates ArcServeIT Disaster Recovery and Dantz Retrospect software, computer systems could be regenerated directly from tape without the need to reload operating systems first, enabling restoration in minimum time. Backup procedures are periodically tested to ensure their functionality in the event of an actual data loss situation. For hard-copy data, including source documents and reports, protection against loss is again provided by a combination of automated/hard-copy data-logging systems. Ultimately, however, logging procedures are only as good as the amount of care taken by staff in recording and checking logs. All current NOVA staff for this project have been selected, because of the nature of the work that NOVA has been conducting, with these attributes in mind. Our perfect record in handling large volumes of data has been due primarily to the meticulous care taken by our staff.

Contingency plan (Level 2)	NOVA's Security Officer and Chief Technology Officer and Director of Network and System Operations have jointly developed contingency plans that are in place in accordance with the DHHS *Automated Information Systems Security Program Handbook* (AISSP), Release 2.0. In the event of extensive fire, natural disaster, or other worst-case catastrophic damage to NOVA's physical premises, a contingency plan has been developed to restore computer systems to full operation within 3 days of a complete loss of existing infrastructure. NOVA maintains agreements with key vendors to provide comprehensive support services during such an emergency situation. All equipment is fully insured at replacement value. Local real estate brokers are prepared to lease comparable temporary commercial space nearby in Bethesda, Rockville, or Silver Spring to accommodate NOVA's personnel and office equipment. These spaces are prewired with Category 5 twisted-pair cable, enabling rapid reconstruction of the corporate network. Gerstel Office Furniture, located in Gaithersburg, Maryland, can supply desks, chairs, bookshelves, storage cabinets, and conference tables in less than 3 business days. Ikon Office Solutions will provide replacement copiers and fax machines within 3 business days. Verizon will provision voice and modem lines within 1 week. Lucent/Avaya will provide a PBX, handsets, and necessary reprogramming within 1 week. Hewlett-Packard will replace all network hardware, including switches and servers, within 1 day. CDW is prepared to deliver new workstations, monitors, printers, and other peripherals by the next business day, including installation of operating systems and key applications if necessary. CDW can also supply skilled temporary personnel to assist with computer setup and reconfiguration. Allegiance Telecom can transfer Web, e-mail, and FTP functions to an offsite hosted environment within 1 day, and reestablish a T1 leased line for onsite Internet connectivity within one week. NOVA has multiyear relationships with each of these vendors, who have consistently demonstrated reliability and responsiveness in critical situations.
Offsite storage—optional (Level 2)	As described above, archival copies of weekly server and monthly individual workstation streaming tape backups are rotated offsite to a secure location suitable for storage of magnetic media.
Audit and variance detection (Level 2)	Activities that require collection, processing, and/or storage of data include integrity controls to ensure that data are not deleted, added, or changed without proper authorization. There are appropriate audit trails allowing the source of all data and/or subsequent changes to be verified. Audit trails are maintained such that the user identifier (and thus, the user) taking an action to add, delete, or change a data record is recorded. This ensures user accountability for actions taken. Interfaces between other systems and networks (e.g., Internet) are regularly examined and appropriate recommendations developed that minimize potential for data compromise.
Maintenance controls (Level 2)	Strict Configuration Management procedures are used to ensure that all authorized software functionality, and only authorized functionality, is incorporated into data processing systems. Systems maintenance tasks that entail functionality modification or involve unrestricted access for any reason are performed only by qualified Systems Administrators. These personnel undergo rigorous background checks, specific training on NOVA systems, and trial evaluation periods before acquiring such maintenance authority.

Physical/environmental controls, including emergency power program and detailed fire emergency plan (Level 2)	NOVA's Security Officer and Chief Technology Officer and Director of Network and System Operations have jointly developed an emergency power program in accordance with the DHHS *Automated Information Systems Security Program Handbook* (AISSP), Release 2.0. NOVA's computers are equipped with uninterruptable power supplies and line-interactive voltage regulation to avoid loss of equipment or data in power outages or power surges. These systems are integrated such that NOVA's servers will automatically perform a clean shutdown in the event of a power failure in excess of 30 minutes and resume operation when the primary electricity supply returns to normal. NOVA's server closet is equipped with enhanced climate control to ensure optimum operating temperature of all critical computing equipment in the event of failure or impairment of the building-wide heating and cooling systems. NOVA's facility is locked 24 hours per day, and all visitors must sign in with the Receptionist and be escorted by a NOVA employee while in NOVA's facility. All major computer equipment (network file server, accounting server) are further secured within locked offices with restricted access on a need-to-know basis only. All NOVA emergency exits are clearly and appropriately marked. All emergency doors open outwards into common exit space that contains open staircases for building egress. Exit doors are locked only for entry, not exit, and automatically lock against suite entry when closed. NOVA's entire facility, including all computer rooms, is protected with fire-suppression sprinkler systems. NOVA's facility is fully equipped and protected with automatic emergency electrical power shutdown controls in the event of fire or other building emergency. NOVA's facility and building management company have posted a Fire Safety Plan, and all employees are oriented to the plan. The building management company periodically conducts emergency evacuations in cooperation with the local fire department. In compliance with the Fire Safety Plan established by the management company, NOVA has an assigned Floor Captain and an Assistant Floor Captain who provide leadership to implement fire exit procedures and two "Searchers" to help make sure all occupants leave the building. If a fire alarm is activated, the Floor Captain and Assistant Floor Captain report to NOVA's reception area and maintain communication with the management office until all occupants have left the floor. The Searchers move throughout the floor, directing occupants to appropriate exits, and report to the Floor Captain when all occupants have been accounted for.
Handling/storage controls (Level 2)	All personal information gathered is kept under lock and key. Data are accessible only to client-authorized personnel for research, monitoring, and audit purposes. All sensitive materials are stored in the locked data management room. All sensitive data are placed in a red folder labeled SENSITIVE DATA. These materials are maintained and stored in NOVA's locked data management room and removed only when in active use. In most instances, information will be used in the data management room, which contains two computers connected to NOVA's network server. Sensitive data will be entered only into password-protected database files. NOVA will shred unneeded sensitive hard-copy documents. There are four shredders conveniently located in NOVA's offices for disposal of confidential and sensitive information. Storage media containing sensitive data are erased

	using multiple write and format cycles in accordance with Federal standards.
Documentation (Level 1)	NOVA's Chief Technology Officer and Director of Network and System Operations maintains all operating system documentation in a locked office. Anyone needing operating system documentation must sign out the books or CDs and sign them in when returned, thus ensuring that the Director always knows the location of any documentation not in the secured office. Whenever operating systems are upgraded, a complete set of current updated documentation is obtained with the upgrade from the manufacturer (e.g., Microsoft). NOVA does not employ any custom operating systems.
Virus prevention measures (Level 2)	NOVA uses memory-resident comprehensive antivirus software packages on its Windows and Macintosh microcomputers to screen all data disks and e-mail attachments. On both platforms, we use Norton AntiVirus, which is updated regularly. In addition to this protection at the desktop, network-based virus filtering is in place as a further safeguard. NOVA uses Computer Associates' InoculateIT to continuously monitor all network traffic, including incoming and outgoing e-mail, for known virus signatures and suspicious virus-like activity. In the event of an infection, this mechanism immediately isolates the infected workstation from the rest of the network and alerts systems personnel via e-mail and pager, preventing spread of the virus and enabling rapid response to prevent potential damage. InoculateIT automatically updates its database every 6 hours, minimizing the threat of newly discovered viruses. By utilizing a dual strategy of protection at both the network and desktop levels, NOVA has been very successful in avoiding virus infections. Finally, NOVA staff are well trained in best practices for handling data files and e-mail attachments originating off site. NOVA staff use these antivirus software packages to electronically screen all data, information, and software provided to the Government before files are sent to the Government. These screening programs include identification and removal of all viruses, worms, and other forms of software infestation known to the providers of these antivirus packages. NOVA staff also utilize these antivirus software applications to screen all data, information, and software obtained from the Government for processing on NOVA's network and personal computers. The Project Manager will immediately notify the agency's Project Officer of any virus, worm, or other form of software infestation found on any Government-provided electronic files. NOVA recommends the use of its current antivirus software applications, which are already installed on NOVA computers. If the Project Officer prefers that NOVA use other antivirus utilities to be standardized with the agency, such software will immediately be purchased and installed.
4. Other Safeguards	
Secure telecommunications (Level 2)	All telco voice lines terminate at a Lucent/Avaya Intuity PBX system. This system is designed for secure operation and is configured to disallow any routing between an incoming and an outgoing connection, preventing misuse of these resources. All outgoing calls must originate from a known extension inside the premises, and toll calls require entry of a designated tracking code for auditing purposes. All telco modem lines terminate at a Shiva LanRover/E, which performs secure authentication for each connection using an encrypted ID and

	password, as described above. All Internet traffic is routed through a single T1 line protected by a packet-inspection firewall. NOVA's internal network is additionally isolated by the use of nonroutable IP addresses from the private Class A pool 10.x.x.x. Thus all Internet requests—both incoming and outgoing—must pass through the firewall in order to be fulfilled. Traffic is continuously analyzed for any anomalous activity patterns or matches to known virus signatures, and all unusual events are logged for review. The firewall itself contains no data, acting merely as a secure and regulated gateway. Compromise of the firewall would not result in a security breach under any circumstances, due to the use of nonroutable addresses by all other computers on the internal network. The only NOVA computers visible on the Internet are those that provide Web, FTP, and e-mail services, which must be publicly accessible in order to function. To ensure the highest levels of security, these machines are connected via the firewall DMZ, where they are still protected from protocol-level attacks by the firewall's filtering mechanism. These servers use the Windows 2000 operating system, currently the most reliable and least vulnerable version of Windows. Security alerts from Microsoft and the SANS Institute are checked daily, and appropriate patches are applied within 1 day of release to allow for testing in a nonproduction environment beforehand. NOVA's e-mail services are as secure as standard POP3, IMAP, and SMTP protocols will allow. Any sensitive information transmitted via e-mail must be encrypted using a 128-bit key. Full support for encrypted e-mail transmission is provided by NOVA's Microsoft Exchange-based e-mail platform. Any regulations regarding international encryption limitations are strictly obeyed.
Hardware/software inventory (Level 3)	NOVA's Chief Technology Officer and Director of Network and System Operations maintains a database inventory of all hardware and software, including its locations, users, and disposition. Record-retention procedures for hard-copy documents and electronic documents, files, and databases are documented and implemented, and annual record-retention reviews are conducted.
Systems personnel availability	All Systems Administrators are required to be available 24/7 for rapid response to any systems outage, security breach, virus infection, or similar critical situation. They are provided with cellular telephones and/or pagers for this purpose. Automated notification systems continuously monitor key computing services and will trigger a warning e-mail and/or page if a monitored service ceases to operate within expected normal parameters. Systems Administrators are equipped with laptop computers in order to perform remote troubleshooting and repair, enabling rapid and convenient recovery under most circumstances.

1.15 Organization Suitability and Assessment:

NOVA Research Company has performed as a central data coordination center for numerous multi-site behavioral research, prevention research, and surveillance studies for CIOs of the Centers for Disease Control and Prevention and for the National Institutes of Health for almost two decades. These studies have been conducted using a variety of modes of administration, including the World Wide Web. NOVA Research, as discussed in NOVA's Security Policy, follows all appropriate DHHS AIS Handbook requirements for handling

personal health information and sensitive data and has never had an incident of data compromise. NOVA's Security Officer and CTO regular conduct data and application program protection assessments and incorporate new technologies, as appropriate to enhance IT security.

1.16 Categorization of Information Sensitivity and System Criticality

TO BE COMPLETED WHEN IDENTIFIED

Requirement	Level
Data Confidentiality (Sensitivity)	
Data Integrity (Sensitivity, Criticality)	
Data Availability (Criticality)	
System Availability (Criticality)	
System Integrity (Criticality)	

2.0 DATA PROCESSING CONTROLS

2.1 Data Classification and Management

TO BE COMPLETED WHEN IDENTIFIED

2.2 Data Inputs

TO BE COMPLETED WHEN IDENTIFIED

2.3 Data Outputs

TO BE COMPLETED WHEN IDENTIFIED

2.4 Outsourcing

NOVA Research provides in-house administrative and system development personnel to maintain and enhance their systems. No outsourcing of any project-related task to another vendor is anticipated, nor would be performed without prior authorization. Based on system requirements, no special security or sensitivity roles are needed.

2.5 Media and Hard Copy Controls

TO BE COMPLETED WHEN IDENTIFIED

2.6 Disposal

TO BE COMPLETED WHEN IDENTIFIED

No paper documents containing any individual record data will be produced. All data will be maintained only in electronic format. Paper documents produced from conduct of statistical analyses of the collected dataset will only contain aggregated data that cannot be identified to any individual or individual data record.

3.0 PERSONNEL SECURITY CONTROLS

3.1 All Users

TO BE COMPLETED WHEN IDENTIFIED

3.2 Administrators and Privileged Users

3.2.1 Access Control/Least Privilege

1. TO BE COMPLETED WHEN IDENTIFIED

3.2.2 Password administration

All users of the system, including administrators, are required to change their password every sixty days. Passwords must be at least eight characters, cannot match the three previously used passwords, and may never be written down or shared with others. Forgotten passwords must be reset to a known value and then immediately changed by the user prior to subsequent access authorization. This policy can be easily modified if necessary to align with particular authentication standards. Upon departure of a system administrator or other person previously authorized to access the system, NOVA's Chief Technology Officer will immediately disable the account in question and revoke all privileges thereof. After a 30-day period of inspection to ensure all essential data has been retrieved from the disabled account, it will be permanently deleted.

3.2.3 Help Desk

Technical support is currently provided by developers who regularly check the support@novaresearch.com e-mail list, and by telephone during normal business hours Monday through Friday, 8 am - 5 pm EST. Outside of this standard schedule, NOVA's Webmaster will be available 24/7 by both pager and e-mail to respond to critical time-sensitive needs from clients and/or project personnel. Non-urgent requests received by the Webmaster will be deferred into the regular daytime support queue.

3.3 User Policies and Rules of Behavior

3.3.1 User Accountability (Addressed in other sections of this questionnaire)

1. TO BE COMPLETED WHEN IDENTIFIED

4.0 ADMINISTRATIVE CONTROLS

4.1 Previous Assessments, Certifications, and Accreditations

TO BE COMPLETED WHEN IDENTIFIED

4.2 Security in the System Development Life Cycle

TO BE COMPLETED WHEN IDENTIFIED

4.3 Documentation

Documentation will be developed as one component of the overall system development effort, before system deployment for data collection.

5.0 OPERATIONAL CONTROLS

5.1 Change Control

TO BE COMPLETED WHEN IDENTIFIED

NOVA maintains valid and current licenses for all software used on both workstations and servers.

5.2 Integrity Controls

TO BE COMPLETED WHEN IDENTIFIED

5.3 System Monitoring

An offsite watchdog sentry that tests basic functionality at five-minute intervals monitors NOVA's Web and database servers continuously. A system administrator is on call 24/7 to respond to critical alerts and repair minor application or configuration issues. In the event of comprehensive software/operating system failure, the system can be rolled back to a previous known good tape image using ArcServe IT Disaster Recovery from Computer Associates within 2-3 hours. NOVA has demonstrated better than 99.9% uptime on all servers and network infrastructure over the past ten years of measurement.

NOVA reserves the opportunity to take the Web site offline for two hours per week in order to perform routine maintenance and security-related updates. These maintenance windows will occur during times when the least amount of client traffic is expected based on analysis of access logs, will be standardized accordingly as much as possible, and all project personnel will be notified which times are so designated. If the site should go offline for more than thirty minutes at any other time, NOVA's System Administrator will automatically be notified via e-mail and pager by offsite operations monitoring software. The System Administrator is available 24/7 to respond to any service outages by whatever means necessary, including soft restart, hard reboot, restoring known good images from backup, etc. If the System Administrator anticipates

that the site will remain down for longer than an additional ninety minutes (approx. two hours total), he will notify relevant project personnel of the outage via e-mail, briefly describing the situation, and providing a best estimate as to when the site will return to normal operation. Additionally, if the primary Systems Administrator is unable to respond for any reason, a backup Administrator with comparable authority will automatically be notified by the monitoring software after one hour of service interruption.

In the event of a system compromise by unauthorized personnel, the system will be immediately taken offline for a brief period of analysis in order to determine the extent of the compromise and the resulting necessary remedies. Once the intrusion vector has been determined and a remedy devised, a known "clean" image of the server will be restored from backup, the security hole will be patched, and the system will be placed back online. NOVA servers are backed up daily, so such a compromise would not result in significant loss of data.

5.4 System Verification

NOVA performs regular conceptual vulnerability assessments of all systems, including evaluating network perimeter protections, access rules, authorized users, and current security status of all hosts. Any potential vulnerabilities identified are remedied as quickly as possible. NOVA does not perform active simulation of potential attacks against its systems, although this expertise is available on staff, if necessary.

5.5 Contingency Planning

See response to 5.6 below.

5.6 Backups, Continuity of Operations, and Disaster Recovery Planning

In the event of extensive fire, natural disaster, or other worst-case catastrophic damage to NOVA's physical premises, a contingency plan has been developed to restore computer systems to full operation within three days from a complete loss of existing infrastructure. NOVA maintains agreements with key vendors to provide comprehensive support services during such an emergency situation. All equipment is fully insured at replacement value.

Local real-estate brokers are prepared to lease comparable temporary commercial space nearby in Bethesda, Rockville, or Silver Spring, to accommodate NOVA's personnel and office equipment. These spaces are pre-wired with Category 5 twisted-pair cable, enabling rapid reconstruction of the corporate network. Gerstel Office Furniture, located in Gaithersburg, Maryland, can supply desks, chairs, bookshelves, storage cabinets, and conference tables in less than three business days. Ikon Office Solutions will provide replacement copiers and fax machines within three business days. Verizon will provision voice and modem lines within one week. Avaya will provide a PBX, handsets, and necessary reprogramming within one week. Hewlett-Packard will replace all network hardware, including switches and servers, within one day. CDW is prepared to deliver new workstations, monitors, printers, and other peripherals by the next business day, including installation of operating systems and key applications if necessary. CDW can also supply skilled temporary personnel to assist with computer setup and

reconfiguration in addition to NOVA's full-time computer infrastructure support staff and Chief Technology Officer. Allegiance Telecom can transfer Web, e-mail, and FTP functions to an offsite-hosted environment within one day, and re-establish a T1 leased line for onsite Internet connectivity within one week. NOVA has multi-year relationships with each of these vendors, who have consistently demonstrated reliability and responsiveness in critical situations.

6.0 TECHNICAL CONTROLS

6.1 Authentication Control

TO BE COMPLETED WHEN IDENTIFIED

6.2 System Access Authorization

TO BE COMPLETED WHEN IDENTIFIED

6.3 Application-Level Protections

TO BE COMPLETED WHEN IDENTIFIED

6.4 Encryption

TO BE COMPLETED WHEN IDENTIFIED

NOVA Research Company

Rules of Conduct

These Rules of Conduct (RoC) provide general instructions on appropriate use of NOVA's IT resources. All NOVA Research Company staff working onsite at a government facility or working on government contracts and grants are required to read this document and sign and submit the accompanying form before accessing Company or government computers and/or networks.

Because written guidance cannot cover every contingency, Company users are asked to augment these rules and use their best judgment and highest ethical standards to guide their actions. Because these principles are based on federal laws and regulations and DHHS regulations and directives, there are consequences for failure to comply with these principles of Conduct. Violation of these rules may result in suspension of access privileges, written reprimand, suspension from work, and criminal and civil penalties.

All NOVA Research staff must sign this form, acknowledging that they have been made aware of and understand the requirements and responsibilities outlined in this document. Questions about these RoC may be directed to one's supervisor or NOVA's Executive Vice President/IT Security Officer, Paul A. Young.

Activities on NOVA network system resources are subject to monitoring, recording, and periodic audits. Authorized IT security personnel may access any "user's" computer system or data communications and disclose information obtained through such auditing to appropriate third parties (e.g., NOVA corporate officers). Use of NOVA's IT system resources expresses consent by the user to such monitoring, recording, and auditing.

Your signed acknowledgement should be submitted to your supervisor or NOVA's Vice President for Human Resources (VP/HR). Each supervisor will be required to file forms with the VP/HR on an annual basis, which will be placed in the respective employee's personnel file. On an annual basis, the VP/HR will be responsible for reporting to NOVA's IT Security Officer the number of personnel who have been authorized to access NOVA systems and the number and percent of whom have signed the acknowledgement form.

The following pages outline the RoC for several key areas of NOVA's Information Security Program. Please note that these lists are not exhaustive.

E-mail

NOVA Research Company-provided e-mail is intended for official use and authorized purposes. E-mail users must exercise common sense, good judgment, and propriety in the use of Company-provided resources. Staff who misuse Company resources in any way may have e-mail privileges withdrawn and may be subject to disciplinary action. Guidance for e-mail use is listed below.

- Limited personal use of Company e-mail services is acceptable as long as it does not affect the mission of the Company and does not conflict with laws, regulations, and policies.
- Personnel using Company e-mail, by their use give passive consent to having their e-mail activities monitored. E-mail contents will not be accessed or disclosed other than for security purposes or as required by law.
- Users shall ensure that e-mail communications are free of viruses through regular screening of incoming e-mail traffic and virus-detection updates.
- E-mail spamming (unsolicited commercial e-mail)—sending or forwarding chain letters, other junk e-mail, or inappropriate messages—is not permitted.
- The sending of threatening, obscene, harassing, intimidating, abusive, or offensive material about others is not permitted.
- The use of abusive or objectionable language in either public or private messages is not permitted.
- The sending of messages in support of a “for profit” activity is not permitted.
- The sending of e-mail messages for the purposes of prohibited partisan political activity is not permitted. Prohibited partisan political activity is any activity restricted under the Hatch Act.
- The transmission of confidential or sensitive information by e-mail, unless protected by Company-approved encryption, is not permitted.
- E-mail software should not be left open on computer systems to prevent unauthorized access and misuse.
- Distribution of unauthorized newsletters is not permitted.

Internet

NOVA Research Company-provided Internet access is intended for official use and authorized purposes. Internet users must exercise common sense, good judgment, and propriety in the use of Company-provided resources. Company staff and users who misuse Comapny resources in any way may have Internet privileges withdrawn and may be subject to disciplinary action. Guidance for Internet use is listed below.

- Limited personal use is acceptable as long as it does not affect the mission of NOVA and does not conflict with laws, regulations, and policies.
- Personnel using Company Internet access, by their use give passive consent to having their Internet activities and actions monitored. Monitoring will not be performed, or its findings disclosed, for reasons other than for security purposes or required by law.
- The act of, or the attempt to, break into another computer or introducing malicious code (e.g., computer viruses, worms, or Trojan horses) is not permitted.
- Certain types of data, such as personal or unauthorized Company owned, or non-Company owned software is not permitted.
- It is not permitted to send, retrieve, view, display, or print sexually explicit, suggestive text or images, or other offensive material.
- The use of another person’s account or identity is not permitted.
- The use of Internet games and chat rooms are not permitted.

Passwords

Passwords are an important aspect of computer security and are the front line of protection for user accounts. Listed below are the password requirements to be used for Company information systems.

- Create passwords with a minimum of eight characters. Use a combination of alpha, numeric, and special characters for passwords, with at least at least one uppercase letter, one lower case letter, and one number.
- Avoid using common words found in a dictionary as a password.
- Avoid obvious readable passwords or passwords that incorporate personal data elements (e.g., user's name, date of birth, address, telephone number, or social security number; names of children or spouses; favorite band, sports team, or automobile; or other personal attributes).
- Change passwords every 90 days.
- Change vendor-supplied passwords immediately.
- Do not reuse passwords.
  - A new password must contain no more than five characters from the previous password.
- Protect passwords by committing them to memory or storing them in a safe place:
  - Do not post passwords.
  - Do not keep a password list in an obvious place, such as under keyboards, in desk drawers, or in any other location where it might be disclosed.
- Change password immediately if password has been seen, guessed or otherwise compromised.
- Keep user identifications (ID) and passwords confidential.
- Do not accept another user's password, even if offered.
- Report, in writing, any compromise or suspected compromise of a password to your supervisor or NOVA's IT Security Officer.
  - All parties shall work to preserve evidence of computer crimes in accordance with Company guidance.

Equipment

NOVA Research Company-provided equipment is intended for official use and authorized purposes. For the Company RoC, there is no distinction between stand-alone and on-line computer systems. Users must exercise common sense, good judgment, and propriety in the use of Company-provided resources. Company staff and users who misuse Company resources in any way may have equipment privileges withdrawn and may be subject to disciplinary action. Guidance for equipment use is listed below.

- Using Company-provided equipment is restricted to business purposes.
  - Limited personal use is acceptable as long as it does not affect the mission of the Company and does not conflict with laws, regulations, and policies; however, keeping family or personal records, or loading unauthorized software onto Company computers is not permitted.
- Personnel using Company equipment, by their use give passive consent to have their use of Company equipment activities and actions monitored. Monitoring will not be performed, or findings disclosed, for reasons other than security purposes or as required by law.
- Equipment, software, or computers using locks or an operating system password should not be reconfigured unless operating under Company-approved and applicable standard procedures.
- Protect passwords, information, equipment, systems, and networks to which a user has access.
- Minimize the threat of viruses by write-protecting diskettes, checking "foreign" data for viruses, and never circumventing the anti-virus safeguards of the system.
- Do not leave desktop or laptop computers unattended without password protecting them.
- Report, in writing, lost or stolen equipment, security incidents, or anything unusual or suspicious immediately to your supervisor or IT Security Officer.

Software Licensing

Copyright laws and the license agreements accompanying the software on Company equipment govern Company users' acquisition and use of software. It is the responsibility of all Company staff and users to protect Company interests in the performance of their duties. This includes responsibility for assuring that commercial software, acquired by Company, is used only in accordance with licensing agreements. Likewise, it is also the Company users' responsibility to assure that any proprietary software is properly licensed before being installed on Company equipment. Local Area Network (LAN) and personal computer (PC) users are not to download LAN-resident software. All Company staff and users should be aware that it is illegal to:

- copy or distribute software or its accompanying documentation, programs, applications, data, codes, and manuals without permission or a license from the copyright owner
- encourage, allow, compel, or pressure, either explicitly or implicitly, operations staff and users to make or distribute unauthorized software copies
- infringe upon the laws against unauthorized software copying because someone requests or compels it
- loan software so that a copy can be made
- make, import, possess, or deal with articles intended to facilitate the removal of any technical means applied to protect the software program.

Furthermore, according to the United States copyright law, persons violating software licensing laws can be subject to civil damages and criminal penalties.

Company software rules are as follows:

- Software will not be modified without the approval of both the development team and the Company Chief Technology Officer (CTO).
- Software will only be issued, and used by, authorized individuals as prescribed by local authority.
- The addition of personal IT resources to existing Company IT resources without written authorization from the CTO is not permitted.
- Security features and controls will be activated when processing data.
- Company staff and users aware of any misuse of Company software shall notify their supervisor, the IT security officer, or the CTO.

Off-Site Computing

Access to Company infrastructure via dial-up or broadband connection poses additional security risks, but may be necessary for certain job functions. Since off-site access is allowed, telecommunication logs and Company phone records will be reviewed regularly and routine spot checks will be conducted to determine if Company business functions are complying with controls placed on the use of off-site access connections. Access to Company networks from off-site locations will be monitored by an audit trail security system.

Company-provided off-site access is intended for official use and authorized purposes. Off-site users must exercise common sense and good judgment in use of Company-provided resources. Company staff and users who misuse Company resources in any way may have off-site access privileges withdrawn and may be subject to disciplinary action. Guidance for off-site access is listed below.

- The Company provides off-site access to personnel for business purposes.
  - Limited personal use is acceptable as long as it does not affect the mission of NOVA and does not conflict with laws, regulations, and policies; however, persons other than the authorized Company user should not be permitted to make use of Company equipment and/or software.
- Personnel using Company off-site access, by their use give passive consent to have their computer activities monitored. Monitoring will not be performed or findings disclosed other than for security purposes or as required by law.
- Company staff and users must adhere to the letter and spirit of all applicable laws, regulations, contracts, licenses, policies, standards, guidelines, business controls, security rules, and other expectations.
- Company staff and users must report, in writing, lost or stolen equipment, security incidents or anything unusual or suspicious immediately to their supervisor, NOVA's IT Security Officer or NOVA's CTO.
- Company staff and users must ensure integrity of data created, accessed, or modified.
- Company staff and users must provide a secure and protected environment for Company data and Company-owned computing resources.
- Company staff and users must apply required safeguards to protect Company records from unauthorized disclosure or damage.

Media Control

Company staff and users must adhere to Company-wide procedures for access, storage, and transportation of all media containing sensitive information. Procedures include completing logs to track deposits and withdrawals of media from on-site storage facilities, libraries and backup storage facilities, and procedures for the proper wrapping and labeling of media to be mailed or couriered, or the eventual disposal of media.

NOVA staff and users who misuse government resources in any way may have media access privileges withdrawn and may be subject to disciplinary action. Guidance for media control is listed below.

- Company staff and users should not leave sensitive information, even temporarily, and should monitor it in the following ways:
  - Company staff and users must keep sensitive material in a secure safe or locked cabinet and return all sensitive information to the safe at the end of each business day.
  - Company staff and users must abide by the physical and environmental protection controls relating to sensitive data that is contained in a media storage vault or library.
  - Company staff and users must turn over, place out of sight, or remove from the screen sensitive information when visitors are present.
  - Company staff and users must sanitize or destroy diskettes and other magnetic storage media that contain sensitive data when they are no longer needed to store the sensitive data.
  - Company staff and users must dispose of both electronic and hard copy media in accordance with Company sanitation and disposal policy.

Voice and Data (Fax) Communication

Comapny-provided voice communication resources are intended for official use and authorized purposes. Company staff and users must exercise common sense and good judgment in the use of all voice communication tools. Company staff and users who misuse Company resources in any way may have privileges withdrawn and may be subject to disciplinary action. Guidance for voice communication is listed below.

- NOVA Research provides voice communication access to personnel for business purposes.
  - Limited personal use is acceptable as long as it does not affect the mission of the Company and does not conflict with laws, regulations, and policies.
- Personnel using Company voice communication and facsimile resources, by their use give passive consent to have their voice communication and facsimile activities monitored. Monitoring will not be performed, or its findings disclosed other than for security purposes or as required by law.
- Attempting to break into another's voice mail (federal or private) is not permitted.
- Sending threatening, obscene, harassing, intimidating, abusive, or offensive material to or about others is not permitted.
- Using abusive or objectionable language in either public or private messages is not permitted.
- Sending messages in support of a "for profit" activity is not permitted.
- Sending or relaying sensitive information over an unencrypted line is not permitted.
- Sending messages for the purposes of prohibited partisan political activity is not permitted. Prohibited partisan political activity is any activity restricted under the Hatch Act.
- Unauthorized government-wide or agency-wide broadcast messages are not permitted; and distribution of unauthorized messages is not permitted.

Physical Security

Physical access points to sensitive facilities, or restricted areas housing information systems that process or display information are controlled during working hours and guarded or locked during nonworking hours. Access authorization will always be verified before granting physical access and unauthorized personnel are denied access to areas containing protected information. Appropriately authorized personnel are granted physical access, with escort if necessary, to facilities. Company staff and users should wear identification badges at all times.

Company staff and users who misuse Company or government resources in any way may have their physical access privileges withdrawn and may be subject to disciplinary action. Guidance for physical security is listed below.

- Only authorized Company personnel are allowed to re-enter sensitive facilities and restricted/controlled areas containing information systems and system/media libraries after an emergency-related event (e.g., fire drills, evacuations).
- Company users not on the access roster for a limited access room or facility must sign in and be escorted the entire time present in the room or facility.
- All Company visitors, contractors, or maintenance personnel must be authenticated through preplanned appointments and ID checks.
- Company staff and users should inform physical security officials when a system's sensitivity level requires additional protections and alert physical security leadership to locations that house sensitive equipment.
- Company staff and users must report immediately, in writing, any theft or loss of sensitive equipment to a NOVA corporate officer.

Disciplinary Action

NOVA Research has established procedures for disciplinary actions for security violations its staff and users commit. These disciplinary actions may be based on the sensitivity of information involved and the number of prior offenses.

The Company has defined remedial actions for employees to include reassignment of work duties, disqualification from a particular assignment, letter of warning, suspension, and/or termination.

It is expected that Company staff and users exercise common sense, good judgment, and propriety in the use of Company and/or government-provided resources. Company staff and users who misuse Company or government resources in any way may be subject to disciplinary action. Guidance for violation handling is listed below.

- Company staff and users must report suspected personnel security violations to a NOVA corporate officer for investigation and recommended disciplinary action.
- Company staff and users are subject to disciplinary actions for security violations specified in security awareness training and these Rules of Conduct.
- The Company may remove staff that commit security violations commensurate with high risk to the Company from any contract, and depending on the security violation, criminal sanctions may also apply.
- Company staff and users who purposely disclose their passwords to others to share or transfer access are subject to disciplinary actions.
- Company users and staff should be alert to developments, such as a drastic change(s) in work habits, which may increase the potential for security violations, whether intentional or accidental.
- Company employees should be aware that any use of the Internet or e-mail that is perceived to be illegal, offensive, or in violation of Company policies or standards can be the basis for disciplinary action up to and including termination and legal action.
- Company staff and users should not allow, encourage, or promote the illegal duplication of software in their possession.
- Company staff and users, who purposely make, acquire, or use unauthorized copies of computer software, may be subject to disciplinary action up to and including termination and legal action.

Incident Reporting Escalation

The Company has established procedures for incident and violation handling that its staff and users might identify to limit any compromises to the Company. Guidance for incident and violation handling is listed below:

- Company users must report, in writing, any of the following incidents to their supervisor and NOVA's IT Security Officer:
  - malicious code: a virus, worm, Trojan horse, or other code-based entity that is either successful or unsuccessful in infecting a host. This category applies to incidents and events.
  - pRoCes and reconnaissance scans: involve searching the network for critical services or security weaknesses.
  - inappropriate usage: a person violates acceptable computing use policies, such as sending spam, email threats, or making illegal copies of software.
  - unauthorized access: a person gains logical or physical unauthorized access to a network, system, application, data, or other resource. This access may include root compromises, unauthorized data alterations, Web site defacements, loss/theft of equipment, unauthorized use of passwords, and use of packet sniffers.
  - denial of service (DoS) attacks: a successful or unsuccessful attack (including Distributed Denial of Service Attacks) impairs the authorized use of networks, systems, or applications by exhausting resources, to include Distributed DoS attacks.
  - other types of incidents include, but are not limited to:
    - alterations/compromises of information
    - adverse site impacts
    - classified system incidents
    - loss or theft of equipment.
- Reporting incidents to your supervisor and the IT Security Officer can be made by phone or email, if followed up in writing.
  - IT Security Officer e-mail address is: PAYoung@NOVAResearch.com
  - Phone number is: (301) 986-1891, extension 110.
- Company users should report these incidents within a 2-hour time frame of the incident occurring.
- All Company users and staff should be trained on appropriate incident-response handling procedures.

Education and Awareness

The Company has established procedures for ensuring its staff and users receive education and awareness training. Guidance on education and awareness is listed below:

- All Company users must receive education and awareness training commensurate with their duties.
- All new Company users of IT systems must receive initial training before being authorized network access and within 60 days of employment.
- All Company users must receive annual refresher training.

SIGNATURE PAGE

All NOVA Research Company staff are required to read the Rules of Conduct and are responsible for abiding by its contents. Violations of the Rules of Conduct or computer policies may lead to disciplinary action, up to and including termination of employment. Signing this form acknowledges your understanding of the requirements for access to Company IT systems and your responsibilities as a system user.

Signatures:

Employee's/User's Name: _____

(Print)

Organization: NOVA Research Company

Employee's/User's Signature: _____

Date Signed: _____

Supervisor's Printed Name: _____

(Print)

Supervisor's Signature: _____

NOTE: Sign and return this form to your supervisor or VP/HR. Make a copy for your records. NOVA's VP/HR will retain your original, signed acknowledgement form in your personnel file.

NOVA Research Company

1. Incident Response Policy and Procedures

This Incident Response (IR) policy and procedures document provides guidelines on what constitutes a security incident, how and to whom an incident should be reported, and what actions should be taken to contain the impact of the incident, restore optimal operations, and prevent recurrence of such incidents in the future.

1.1 Goals

The goals of an incident response program are:

- **Quick recovery**. Establishing best practices for developing and implementing an incident response capability in accordance with company policy, procedures, and standards to recover from security incidents quickly and efficiently.
- **Impact minimization.** Implementing an incident response program to minimize loss or theft of information and reduce the effects of a disruption of critical computing services when incidents occur.
- **Systematic response.** Developing appropriate procedures to ensure appropriate, effective, and consistent response to incidents and appropriate evidence collection and preservation.
- **System protection.** Establishing ability to detect and respond effectively to, a security incident in order to protect the confidentiality, integrity, and availability of NOVA Research Company systems and data.

1.2 Personnel

As NOVA Research Company is a small business comprised of a small number of key systems administration personnel, there is no need for a complicated hierarchy of notification, response, assessment, mitigation, restoration, and analysis teams. So we will consider that there are essentially three classes of personnel who interact with NOVA systems. “Users” simply act as clients of system resources, with little or no permissions to change any of the operational or architectural aspects of the system. “Developers” implement applications and program interfaces for Users to access and manipulate data, but do not have authority to modify operating-system (OS) functions. “Administrators” are responsible for maintaining hardware, configuring OS environments, ensuring availability of critical server resources, and protecting data integrity. The NOVA Chief Security Officer (CSO) oversees security considerations for these three groups of personnel, setting policy and receiving reports from Users, consulting with Developers so that their applications conform to security best practices, and working with Administrators to ensure proper prevention measures, detection mechanisms, and repair solutions are in place to deal with potential incidents.

1.3 Definition

There are two basic aspects to IR: prevention and reaction. Prevention involves all of the potential defenses against the occurrence of an incident. Reaction involves the full range of options to restore normal operation of a compromised system. To begin exploring prevention and reaction in detail, we must first identify the types of incidents that we are

prepared to manage. In this document we will exclude consideration of system interruptions due to fire, flood, extended electrical outage, or other catastrophic results of natural disasters or acts of war. Here we will focus primarily on non-physical impacts of malicious human intent, including the following types of incidents.

1.4 Types of Incidents

A security incident is the violation of an explicit or implied security policy in a computing or telecommunications system or network.
The following subsections describe the general categories of security incident.

1.4.1 Malicious Code Incidents

Malicious code refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the security or integrity of the victim's data. Generally, malicious code is designed to perform these functions without the system user's knowledge. Malicious code attacks include attacks by viruses, Trojan horses, worms, mobile code, and blended.

1.4.1.1 Viruses

A virus is designed to self-replicate; make copies of itself; and distribute the copies to other files, programs, or computers. Viruses insert themselves into host programs and propagate when the infected program is executed, generally by user interaction (e.g., opening a file, running a program, clicking on a file attachment). Viruses have many purposes; some are designed to play annoying tricks, whereas others have destructive intent. Some viruses present themselves as jokes while performing secret destructive functions. Categories of viruses include file infector viruses, boot sector viruses, macro viruses, and hoax viruses:

- **File Infector Viruses –** attach themselves to executable programs, such as word processors, spreadsheet applications, and computer games. When they have infected a program, they propagate to infect other programs on the system and other systems that use a shared infected program. The virus also may reside in the system's memory, so that each time a new program is executed, the virus infects the program. Another method of file infector execution involves the virus modifying the manner in which the computer opens a file, rather than modifying the actual program running the file. In this scenario, the virus executes first, and then the program is run. Jerusalem and Cascade are two of the best-known file infector viruses.
- **Boot Sector Viruses –** infect the master boot record (MBR) of a hard drive or the boot sector of removable media, such as floppy diskettes. The boot sector is an area at the beginning of a drive or disk where information about its structure is stored. They are easily concealed, have a high rate of success, and can harm a computer to the point of complete inoperability. Symptoms of a boot sector virus infection include a computer that displays an error message during booting or cannot boot. Form, Michelangelo, and Stoned are examples of boot sector viruses.
- **Macro Viruses –** attach themselves to documents such as word processing files and spreadsheets. As the name implies, a macro virus uses an application's macro programming language to execute and propagate. Many popular software packages, such as Microsoft Office, use macro programming languages in their products to automate complex or repetitive tasks. Attackers have taken advantage of macro programming capabilities to distribute malicious code. Macro viruses tend to spread quickly because users frequently share documents from applications with macro capabilities. Furthermore, when a macro virus infection occurs, the virus also infects the template that the program uses to create and open files. Consequently, every document that is created or

opened with the infected template is also infected. The Concept, Marker, and Melissa viruses are examples of macro viruses.

- **Hoax Viruses –** are false virus warnings. The phony viruses are usually described as being of devastating magnitude and requiring immediate action to adequately protect computer resources from infection. Despite the illegitimacy of their messages, hoax viruses are just as prevalent in the digital world as actual viruses. They are circulated by innocent end users who believe they are helping by distributing these warnings to the Internet community. They usually cause little damage, although some malicious hoax viruses direct users to alter operating systems settings or delete files, which may cause security or operational problems. They can be time consuming, as many of the hoax recipients may contact technical support staff to warn them of the new threat or to ask for guidance. Good Times and Bud Frogs are examples of hoax viruses.

1.4.1.2 Trojan Horses

A Trojan horse is a program that appears legitimate (e.g., a game or utility program), but performs some illicit activity when run. The program may be used to locate password information, to make the system more vulnerable to future entry, or simply to destroy programs or data on the hard disk. A Trojan horse is similar to a virus, except that it does not replicate itself and it remains in the system performing damage or creating a backdoor for remote access to the system.

1.4.1.3 Worms

A worm is a self-replicating program that is completely self-contained, meaning they do not require a host program to infect a victim. The main destructive property is using up a computer's resources, degrading system performance, or shutting down the system completely. Worms also sometimes write unusual messages to indicate their presence. Worms generally propagate themselves over networks or replicate through electronic messaging and thus, can spread very quickly.

1.4.1.4 Mobile Codes

Mobile code is software that is transmitted from a remote system to a local system and then executed on the local system without the user's explicit instruction. They often act as a mechanism for a virus, worm, or Trojan horse to be transmitted to the user's workstation. In other cases, mobile code takes advantage of vulnerabilities to perform its own exploits, such as unauthorized data access or root compromise. Popular vehicles for mobile code include Java applets, ActiveX, JavaScript, and VBScript.

1.4.1.5 Blended Attacks

A blended attack is an instance of malicious code that uses multiple methods to spread such as:

- **E-mail**. A user on a vulnerable host opens an infected e-mail attachment; a blended attack looks for e-mail addresses on the host and then sends copies of itself to those addresses.
- **Windows shares**. A blended attack scans hosts for unsecured Windows file shares; it can then use NetBIOS as a transport mechanism to infect files on that host in the hopes that a user will run an infected file, which will activate the blended attack on that host.
- **Web servers**. A blended attack scans Web servers, looking for known vulnerabilities in Microsoft Internet Information Server (IIS). If it finds a vulnerable server, it attempts to transfer a copy of itself to the server and infect it and its files.
- **Web clients**. If a vulnerable Web client visits a Web server that has been infected by a blended attack, the client's workstation will become infected.

In addition to using these methods, blended attacks may spread through other services, such as instant messaging (IM) and peer-to-peer (P2P) file sharing. People tend to refer to most instances of blended attacks as worms.

1.4.2 Probes and Scans

Probes and reconnaissance scans involve searching the network for critical services or security weaknesses. These scans are normally the first step a hacker will take in trying to penetrate a network, since it allows a hacker to identify network services, operating systems, and applications in addition to the network topology.

1.4.3 Unauthorized Access

Unauthorized access involves improper use of a valid account or unauthorized access to files and directories stored on a system or storage media. Unauthorized access also could entail access to network data by planting an unauthorized network "sniffing" program or device to capture all information traversing the network at a particular point.

1.4.4 Improper Usage

Often a corollary to unauthorized access, improper usage encompasses the use of data, services, and other resources for reasons that are expressly forbidden by NOVA policy or procedure. For example, a user (or a hacker impersonating a user) might access company IT resources to gather information or perpetrate an attack on a system or network. Unauthorized information resource activities include:

- Conducting unlawful, disruptive, or other malicious activities within or outside a NOVA computing environment;
- Displaying or printing material or images that are sexually explicit, discriminatory, or harassing in any way;
- Using abusive language in transmitting public or private messages;
- Sending inappropriate e-mails, virus and other e-mail hoaxes, chain letters, and pornography;
- Surfing the Web at inappropriate sites; and
- Using a computing system for other than sanctioned purposes.

1.4.5 Denial of Service

A Denial of Service (DoS) attack is one where a hacker or a malicious code disrupts or halts a service by overloading a crucial functional component, such as overwhelming a Web site with illegitimate requests. Given their relatively simple execution, DoS attacks have grown increasingly popular with novice hackers and have posed significant challenges to a number of Web sites and networks.

The goal of a DoS attack is to cripple a device or network so users no longer have access to resources, which can be accomplished by exhausting or crashing a resource. Distributed Denial of Service (DDoS) attacks are usually launched from multiple sources, all targeting a specific victim. Attacks can be initiated by individuals or automatically executed by programs known as "zombies." Zombies are installed on host computers before the attack and executed by special embedded code or a signal sent by an individual. This method helps disguise the identity of the attacker because the attack itself is coming from completely unrelated computers.

1.4.6 Unauthorized Alterations/Compromises of Information

Unauthorized alterations or compromise of information could involve an individual (including authorized and unauthorized users) who either inadvertently or intentionally changes, releases, or steals information.

1.4.7 Loss or Theft of Resources

The loss or theft of NOVA IT resources, which includes physical equipment like computers and smart cards, as well as intangible resources such as passwords, can present a serious threat to overall NOVA security. These events must be immediately reported to the NOVA CSO to determine the potential compromise of sensitive material.

1.5 Establishing an Incident Response Capability

An incident response capability is a means for effectively preparing for and reacting to IT security incidents, reporting incidents to proper authorities, and preserving the ability of NOVA Research Company to fulfill its mission. The incident response capability must not only react to incidents, but it also must have the resources to alert and educate users to pertinent risks and heighten awareness about security threats and incident-handling procedures. NOVA supports a six-stage process to establish an incident response program. The six stages are illustrated in Figure 1. Understanding each stage facilitates a more efficient and methodical response to incidents from all levels of the NOVA work force.

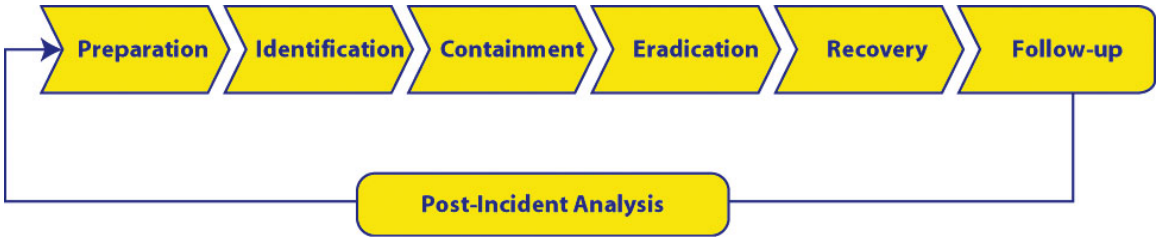

Figure 1. Incident Response Process

1.5.1 Preparation Phase

One of the most critical aspects of responding to security incidents is adequate preparation. Preparation limits the potential for damage by ensuring that response personnel have understood and practiced incident response activities before an event occurs. Without preparation, response efforts may become disorganized, confused, inefficient, and ineffective. The following are a list of best practices used by NOVA Research during the preparation phase:

- **Responsibilities.** Roles and responsibilities are identified and assigned
- **Security policies.** All security policies relating to incident response, especially those on the authorized and unauthorized use of information resources, secure account use, secure password management, and disciplinary or corrective actions for noncompliance, are regularly reviewed and fully implemented.
- **Security procedures.** Security procedures, such as incident response and recovery, system integrity checks, network and system change management processes, network and system security incident reporting, report review procedures, security patch implementation, and account expiration, have been developed and documented.
- **Management support. NOVA m**anagement fully supports this incident response policy and procedures and works with the CSO and CTO to coordinate oversight for incident response.
- **Incident response support infrastructure.** A contact list of key security personnel, as well as additional staff that may provide additional expertise, is essential for rapid response. Emergency action plans and checklists have been established to assist in the response effort. Similarly,

resources of appropriate response software and tools (e.g., “jump bags” with compact discs (CDs), floppy disks, screw drivers, manuals) are readily available to assist in the response effort.

- **Information recovery.** System and data backups and recovery procedures are established and regularly tested. Regular backup of system data helps ensure operational continuity. Such backups facilitate information recovery during an emergency, especially in cases where incident response teams include personnel that are not normally assigned to a particular system or network.
- **Network security.** All NOVA systems and networks have protections installed that are commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.
- **Software tools.** Incident mitigation, prevention, and detection tools are installed and appropriate staff members are trained on their proper use. The use of technical tools, such as antivirus programs and intrusion detection monitoring software, can greatly enhance incident response capabilities.Incident-response tools are implemented and testing and training are regularly conducted .
- **Notification & communication.** All authorized system users are aware of notification procedures in the event of an incident. NOVA management and key security personnel contact information is readily accessible to facilitate rapid incident reporting.
- **Training.** All NOVA personnel (including contractors, if applicable) have been trained on IT security incident response and reporting. New personnel are trained immediately after hiring.
- **Law enforcement & public relations.** Procedures are established that clearly govern interactions with law enforcement, the public, and the press.

1.5.2 Identification Phase

Identification involves determining whether an incident has occurred and defining the incident. For example, identification normally begins after an anomaly in a system or network has been noticed. It is the responsibility of a NOVA Systems Administrator to determine the validity of an incident. Verification of the incident is critical to conducting an effective response. Indicators that may indicate that a security incident might have occurred include the following:

- System reboots;
- Poor resource performance;
- Web page defacement;
- A system alarm or notification or log review and analysis results from a detection tool, (e.g., antivirus software or intrusion-detection systems);
- Probes and reconnaissance scans;
- Suspicious entries in system or network logs (e.g., a UNIX user obtains root access without following the standard process for obtaining such access);
- Accounting discrepancies (e.g., indication of an 18-minute gap in the accounting log suggesting log tampering);
- Unsuccessful logon attempts and unexplained new user accounts;
- Unexplained new files, unfamiliar file names, modifications to file lengths and dates, especially in system executable files;
- Unexplained attempts to write to system files or changes in system files;
- Unauthorized access and use of a system for processing or storing data;
- Disruption or inability of one or more users to login to an account;
- Unusual system performance or behavior, including system crashes, degraded performance, or suspicious component outages;

- Unauthorized operation of a network traffic analyzing program or sniffer device;
- Use of attack network scanners, remote requests for information about systems and users, or similar social engineering attempts;
- An indicated last time of usage of a user account that does not correspond to the actual last time of use for that user;
- Abnormal delay in network or application services;
- Unauthorized changes to system hardware, firmware, or software characteristics;
- Missing data, files, or programs;
- Unexplained modification or deletion of data;
- Unauthorized use of services;
- Unexplained or unusual after-hour system activity;
- Security policy violations;
- Routine malicious code events;
- Unauthorized privileged user activity;
- Unexplained access privilege changes;
- Unexplained activities that are present in the system activity or system logs review; and
- Unusual usage patterns (for example, programs are being compiled in the account of a user who does not know how to program).

1.5.2.1 First Response Handling

Often, the first moments of a security incident provide unique opportunities for gathering information and analyzing the attack. Once NOVA personnel believe that an incident is in progress, the following steps will facilitate stronger responses from security personnel and other involved groups:

- **Remain calm.** Take the time to follow all steps to handle the incident properly. Rushing may cause mistakes.
- **Respond immediately.** Immediately record any evidence of the incident before it has been altered. Waiting to respond can result in lost or tampered evidence.
- **Make duplicates.** Make copies of the registers, cache contents, memory contents, state of network connections, state of running processes, contents of the storage media, and contents of removable and backup media.
- **Keep detailed notes.** Take systematic notes and write down observations with time stamps as the incident response progresses. Do not try to remember everything.
- **Use a tape recorder.** A tape recording of the conversations and interviews conducted during an incident will not only strengthen the incident log, but may also support subsequent law-enforcement investigations and criminal prosecutions.
- **Preserve evidence.** A sound forensic technique must be used to preserve evidence. Once evidence is gathered, chain of custody must be observed to take the next steps.
- **Leave the system in its current state.** For investigative purposes, it is imperative that the system remains in the same state that it was in when the incident was discovered. Do not install additional programs, since doing so might overwrite potential evidence on the system.
- **Notify the appropriate individuals.** Management needs as much information as possible to make the best decisions. Incidents that are in progress or appear to be accelerating in intensity and frequency should be reported immediately. All NOVA system users (including contractors) should report incidents immediately to their System Administrator, CSO, or a NOVA corporate officer.

1.5.2.2 Identification Actions

Once a security incident has been identified, the following actions should be taken:

- **Scope determination.** Determining the scope of the incident enables security personnel to establish and prioritize response activities. A System Administrator will determine the scope and breadth of the incident, including resources affected by the incident, how they were affected, and what impacts the incident may have on other systems. This action requires an effective communication process that enables the System Administrator to collaborate with technical and managerial knowledge leaders across the organization.
- **Analysis.** The level of detailed analysis required will vary, depending on the type of incident and the resources affected. Because of the potential need to conduct complex investigations, NOVA incident response teams (IRTs) are composed of persons with specific infrastructure, system, and network technical skills. It is often necessary to apply these skills to an event to analyze efficiently and effectively the sequence of events and logs associated with the incident under analysis.
- **Information recovery.** Full system backups help preserve the state of the original computing environment and provide a baseline for subsequent research and analysis. Perpetrators of computer crime may attempt to destroy evidence of their activities. Without a full backup, the evidence may be destroyed before the IRT members can examine the data. All backup tapes are stored in a secure location to prevent damage and theft and are regularly removed to off-site storage.
- **Incident log.** It is vital to maintain a detailed incident log during the identification phase. The incident log should include the name of the system, time, and other relevant details about the event, such as the names of the IRT members and details of IRT response activities. Careful recording of these facts can assist efforts in identifying the type of incident, developing effective solutions, and prosecuting those who commit computer crime. The incident log will be secured with access granted only to authorized personnel.
- **Tools.** Software tools help to identify incident facts and indicators. Antivirus tools detect, eliminate, or quarantine viruses. Intrusion-detection tools can identify unauthorized access or use. System and network audit logs also provide information on the validity of a security incident. The IRT regularly assesses and deploys such tools to protect NOVA resources, in accordance with NOVA policy and the requirements of the resources being protected.
- **Incident response tool notification.** Many intrusion detection systems and tools are equipped to generate alarms when a suspect activity or violation occurs. These systems can call a designated phone or pager number, send e-mail to a designated e-mail account or accounts, or send a real-time notification message to a designated computer. NOVA system and network administrators have configured intrusion-detection systems to notify appropriate IRT personnel and to maintain a log entry of the event. There is always be a knowledgeable staff member observing the information coming in to determine false positives before notification is initiated.
- **External notification.** IRTs will coordinate external notification with US-CERT, law enforcement, and other external entities through the NOVA CSO.
- **Response coordination.** One IRT member is designated as the incident handler to coordinate the incident response. The IRT is augmented with additional NOVA personnel (e.g., security manager, human resources, legal, and system administrators) as needed. Public affairs personnel are notified of the incident, as appropriate, from the IRT. All personnel are instructed not to talk directly to representatives from the media or law-enforcement authorities.

Table 1 summarizes these identification actions.

Scope Determination	• Determine scope and breadth of incident • Include resources affected and how affected • Consider systems that trust the affected system
Analysis	• Determine whether event is a computer-security incident • Level of detailed analysis will vary depending on situation
Information Recovery	• Obtain full backup of system being observed • Preserve state of computing environment • Store backup tapes in a secure location
Incident Log	• Maintain incident log of suspicious events • Include name of system, time, other relevant details • Secure log with access granted to authorized personnel only
Tools	• Software tools, antivirus tools, intrusion detection tools • Capture audit information, accounting data, logs
Incident Reponse Tool Notification	• Many incident response systems and tools generate alarms • Can contact designated phone, pager, e-mail, or send message • Generate and retain log entry of event
External Notification	• Coordinate external notification through NOVA CSO
Response Coordination	• Designate one member of IRT as incident handler • Augment IRT with additional NOVA personnel • Notify public affairs personnel of incident • Instruct personnel not to talk to media or law enforcement

Table 1. Identification Actions

1.6 Containment Phase

The primary goal of containment is to limit the scope and magnitude of a security incident and to avoid a serious breach of security, information, or infrastructure disaster. To contain a security incident, the following actions will be taken:

- **Resource preservation.** The IRT will determine whether the compromised system should be shut down, disconnected from the network, or allowed to continue normal operations. The answer depends on the type and magnitude of the incident. For example, for a virus incident, the virus can often be quickly removed without disrupting system operations. This decision will be made through authorized NOVA management, in coordination with IRT staff, and will consider the ramifications for resource damage and law-enforcement activities.
- **Incident log.** IRT members will continually maintain and update the incident log throughout the containment phase. The log should include the conditions, issues, and resolutions associated with information protection, scope determination, and all of the containment steps that were initiated. The log will include actions taken, time action was performed, observations, and staff involved. Attention to detail will provide concise, accurate reference data during subsequent incident response phases and review. Accurate maintenance of the incident log can also assist efforts in prosecuting those who commit computer crime.
- **Notification and communication.** The IRT lead will provide all appropriate personnel and management with periodically updated information.

Table 2 illustrates the three containment actions.

Resource Preservation	• Determine whether the compromised system should be shut down, disconnected from the network, or allowed to continue normal operations so that any activity on the system can be monitored.
Incident Log	• Update incident log throughout containment phase • Include conditions, issues, resolutions associated with information protection, scope determination, and containment steps.
Notification and Communication	• Continue to update all parties, to include management, periodically

Table 2. Containment Actions

1.7 Eradication Phase

The goal of the eradication phase is to eliminate the cause of an IT security incident. Eradication actions to be taken may include some or all of the following, as deemed appropriate by the IRT:

- **Communication notification.** The IRT will decide when and how much to advise NOVA system users of the status of compromised systems or other incident-related situations and to request users to assist with the eradication effort. NOVA system users, including contractors, are expected to cooperate with IRT members in handling an IT security incident. At this stage, steady lines of communication will be established between the IRT and NOVA management.
- **Incident log.** IRT members will update the incident log, as appropriate, to record response actions and any challenges that ensue. The log will include the conditions, issues, and resolutions associated with affected computing areas, scope determination, and all eradication steps that were initiated. The log will include the time the action was performed, actions taken, observations, and staff involved. Careful recording of these details will ensure accurate details of eradication efforts taken and serve as reference data during subsequent incident response phases, review, and prosecution. As with all logs of this type, the incident log will be stored in a secure manner.
- **Incident response tools.** Software tools are helpful and often essential when removing all causes of an incident from the computing environment. It is important that the IRT members research and rely on all available audit information, accounting data, and network and system logs to eradicate all instances of the cause of the incident effectively.

Table 3 illustrates the three eradication actions.

Communication Notification	• Advise users of status of compromised systems or other incident-related situations • Users assist IRT members with any events or activities • Establish communication between IRT and NOVA management
Incident Log	• Update incident log as appropriate • Include conditions, issues, resolutions associated with affected computing areas, scope determination, and eradication steps • Store log in a secure manner
Incident Response Tools	• Use software such as virus and intrusion detection tools, in removing causes of incident • Rely on and research all available audit information, accounting data, network and system logs

Table 3. Eradication Actions

Corrective action measures prevent reoccurrence of an incident and aid in returning the system to a secure operating state. The following measures will be implemented as appropriate to facilitate this process; however, they may not be applicable to all incidents:

- Reinitializing system or network logs to establish a clean event log environment;
- Removing unexplained or unauthorized new user accounts;
- Replacing files or executables that reflect unexplained modifications to file lengths or dates;
- Correcting any denial of service impediments affecting accounts or network entry points;
- Eliminating impediments that generate system crashes or poor system performance;
- Implementing corrective or preventive measures prohibiting unauthorized network traffic analyzing programs or sniffer devices;
- Reinitializing affected system hardware, firmware, or software;
- Restoring missing data, files, or programs;
- Removing malicious code from the affected environment; and
- Correcting or removing unauthorized privileged user capabilities and unexplained access privilege changes.

1.8 Recovery Phase

Recovery restores a system to its normal mission status. It is essential to determine the integrity of the backup itself before restoration. Once the system has been restored, it will be validated as well, thus proving that the system is back to its normal condition. The following actions will take place to facilitate recovery:

- **Notification and communication.** NOVA management will be advised regularly of the status of compromised systems, information, or other incident-related situations. The IRT may direct system users to use data backup software to restore data to a point before the security breach. In some cases, associated managers may determine if any data has been compromised or is otherwise unreliable, and whether the data should be destroyed. Any decisions requiring this type of action will be coordinated with the appropriate managers, administrators, and system users. The IRT may also need to notify the user base when the incident has been resolved.
- **Procedures.** IRT members, network administrators, and system administrators will execute the recovery procedures developed and documented during the preparation phase to restore the computing environment after the security incident. Restoration and security procedures, including system integrity checks, network and system change management processes, network and system event security reporting, report review procedures, patch management, and account expiration will be executed at the direction of IRT members, network administrators, and system administrators at this time.

If any accounts have been compromised:

- System administrators will reestablish all authorized accounts and passwords.
- Personnel will be notified at once to change their account passwords.
- Users will be required to reestablish strong passwords on all systems to which they have access, particularly if they use the same or similar passwords on these systems.

If root access has been compromised:

- The operating system (OS), including all applicable patches and upgrades, will be reloaded from trusted media. Security patch implementation and management is also essential at this stage.
- A strong new root password will be set.
- The privileged accounts that had been compromised will be securely reestablished.
- The formerly compromised computer will be reconnected to the network.

Table 4 illustrates the recovery phase procedures.

If any accounts have been compromised…	• System administrators will reestablish all authorized accounts and passwords. • Personnel will be notified at once to change their passwords. • Users willreestablish strong passwords on all systems to which they have access, particularly if they use the same or similar passwords on these systems.
If root access has been compromised…	• The operating system (OS), including all applicable patches and upgrades, will be reloaded. • A strong new root password will be set. • The privileged accounts that had been compromised will be securely reestablished. • The formerly compromised computer will be reconnected to the network.

Table 4. Recovery Procedures

- **Incident log.** It is important to continue logging information during the recovery phase. IRT members will update the incident log to record flaws or events that have been identified and resolved, including methods of correction. Logs will include actions taken, time action was performed, observations, and staff involved. An accurate incident log will ensure accurate details of recovery efforts taken and serve as reference data for post-incident review and prosecution, if applicable.
- **Network security.** Following an incident, NOVA management will review all antivirus, firewall, and intrusion-detection systems and procedures and update them as required. In addition, hardware components will be inspected and repaired or upgraded as necessary. Security patch implementation and management is also essential at this stage. Vulnerability scans will be run to ensure all vulnerabilities are patched or mitigated appropriately.

Table 5 illustrates the four recovery actions.

Notification and Communication	• Advise NOVA management of status of compromised systems, information, other incident-related situations • Direct system users to restore or possibly destroy data • Communicate other important messages to community
Procedures	• IRT, network, and system administrators execute recovery procedures, including system integrity checks, change management processes, event security reporting, report review procedures, patch management, account expiration
Incident Log	• Continue logging information during recovery phase • Record flaws or events that have been identified and resolved, including methods of correction, conditions, issues, and resolutions, scope determination, and all recovery steps
Network Security	• Review all antivirus, firewall, and intrusion detection systems and procedures and update as required • Inspect and repair/upgrade hardware components as necessary • Implement and manage security patches

Table 5. Recovery Actions

1.9 Follow-Up Phase

Although a successful recovery phase usually indicates a return to normal operations, NOVA management is aware that effective follow-up is necessary to ensure that the security incident does not reemerge. Follow-up activity is one of the most critical incident-response activities, because it enables organizations to improve their incident-handling procedures and support any efforts to prosecute perpetrators. The following actions could take place to help simplify the follow-up phase:

- **Procedures.** IRT members, network administrators, and system administrators will continue to monitor event logs to ensure that no further system exploits are occurring, either through the previous vulnerability or through a previously unknown vulnerability. It is essential that a thorough and regular search be conducted to detect any new symptoms or compromises that may have occurred. The IRT and administrators will carefully analyze logs to determine how the incident occurred and what remedial actions are necessary. Once the system has been fully restored and tested, the affected systems will be backed up and securely stored for later use.
- **Incident log.** The recording process will be completed and any outstanding issues or questions resolved and documented.
- **Network security.** NOVA management should ensure that a follow-up search is conducted for hacker programs or files that may have been left behind on the affected system or neighboring systems. If suspicious programs or files are found, the origin of these files will be checked. If any are owned by the root account (or root-privileged accounts), significant system compromises may need to be resolved. Regular network scans will be conducted on all systems to detect vulnerabilities or instances of compromise. If vulnerable services are discovered, NOVA management will take appropriate action to minimize impact of the vulnerabilities.
- **Notification and communication.** NOVA management will, through the appropriate reporting structure, maintain open communications with all relevant external organizations. As appropriate, US-CERT personnel will be updated regularly on incident resolutions and subsequent actions. These updates will include the status of compromised systems, follow-up procedures, or other incident-related situations.

1.10 Post-Incident Activities

Once an incident has been resolved, an in-depth analysis of the incident and NOVA response procedures can lead to developing lessons learned, as well as possible improvements or modifications to the existing IR process. Incident analysis will focus on the events that occurred and how NOVA and supporting organizations reacted to the incident. When conducting incident analysis, all stages of the incident, from preparation to follow-up, will be analyzed. A number of questions should be answered in conducting this analysis, such as:

- Was there sufficient preparation for the incident?
- Did detection occur promptly or, if not, what delayed detection?
- Could additional tools have helped the detection and eradication process?
- Was the incident sufficiently contained?
- Was communication adequate, or could it have been better?
- What practical difficulties were encountered?

Table 6 illustrates these post-incident response questions.

Post-Incident Analysis	• Was there sufficient preparation for the incident? • Did detection occur promptly, or, if not, why not? • Could additional tools have helped the detection and eradication process? • Was the incident sufficiently contained? • Was communication adequate, or could it have been better? • What practical difficulties were encountered?

Table 6. Post-Incident Analysis

Other incident-specific questions also will be addressed during this analysis. The results of the analysis will be documented and incorporated into future operations. As necessary, NOVA policies and procedures will be updated to reflect any lessons learned because of the incident.

1.10.1 Cost Analysis

In determining the effectiveness of the incident response, a detailed cost analysis will be conducted to identify areas for improvement or increased efficiency. This analysis will assist NOVA management in allocating resources for future incident-response operations. In addition, it assists the IRT in streamlining operations and improving organizational efficiency. Successful analysis relies upon the quality and quantity of the data that is collected and used in the analysis, such as:

- Amount of personnel time required to deal with the incident (including time necessary to restore systems);
- Monetary costs associated with resolving the incident and/or any associated impacts of the incident;
- Opportunity costs from lost data and disruptions with ongoing operations; and
- The extent to which hardware is damaged and the impact on operations.

Deriving a financial cost associated with an incident not only will help those who may be prosecuting any suspected perpetrators, but it also will help justify any supplemental budget requests.

1.10.2 Report Preparation

Details from the incident and cost analyses will be incorporated into a final report, which is to be approved by the NOVA CSO and CTO before dissemination to appropriate members of NOVA management. All IRT members associated with the incident will sign the report.

1.10.3 Policy and Procedure Revision

Lessons learned contained in the report may be used as the basis for identifying weak or flawed incident response policies and procedures. NOVA management may need to revise policies and procedures to address shortfalls or to address incidents using innovative technology or techniques. Developing effective policies and procedures is an iterative process in which feedback from follow-up activity is essential.

1.10.4 Performance Measures

Various laws, regulations, and executive guidance require government contractors to measure their performance in preserving the security of IT resources. They are also required to conduct risk assessments and develop corrective plans for improving the

security of their IT resources. Statistics and measurements on security incidents are a critical component of performance measurements and risk assessments. NOVA will develop and produce quarterly and annual statistics on the basis of data gathered as a result of regular reviews and assessments.