Attachment C. AIR's Security Policies for Hosting External Systems

A. Application System Identification

A.1. Application System Category

The American Institutes for Research (AIR) uses the WebSurveyor tool to conduct online surveys. WebSurveyor is a commercially available survey development and implementation tool made available to all AIR programs through its Web Hosting Services group.

AIR chose WebSurveyor after considerable research on available Web-based survey tools. A key reason for this choice is that AIR hosts the application. The tool resides at AIR, on its servers, behind its firewalls and under the protection of its overall security system. This was deemed to be superior to utilizing an externally hosted survey application, where data security is outside the control of AIR and subject to unknown variables.

WebSurveyor also was chosen because it satisfies a variety of needs. It is user-friendly and relatively simple to configure and deploy. It allows for multi-tenancy in that different projects' data can be isolated from each another within the same application. It also integrates easily with AIR's broadcast e-mail system—Lyris—which will be used to send out solicitation e-mails for the survey.

WebSurveyor is part of an array of applications used for AIR's clearinghouse activities. Other applications making up this array include Microsoft GP Inventory and Distribution system integrated with Lyris (broadcast e-mail) and Microsoft CRM. This array includes an eCommerce system used for inventory and distribution management of National Heart, Lung, and Blood Institute (NHLBI) publications. This infrastructure is used to maintain the NHLBI Online Catalog and the NHLBI Integrated Publications system. Working in harmony, these components constitute a major application that secures survey results, orders, inquires from the general public, personal contact information, inventory data, and billing information.

A.2. Security for WebSurveyor

Multiple concentric layers of security (MCLS) is a concept implemented by high-end hosting facilities as well AIR's Web Hosting Services. The concept relies on implementing more restrictive layers until access to actual information is granted. As a hosted application, WebSurveyor is deployed within AIR's MCLS environment.

The model implemented defines the following layers:

Layer 1: Enclaves

We identify and group systems that have similar protection requirements, increasing protection. We have multiple networks. Our internal security enclaves are based on the sensitivity of the information resources resident in each and the assessed threats to those resources.

Layer 2: Border Firewalls and Intrusion Prevention Systems
We use application-layer firewalls to manage access on the Internet perimeter and between intranet enclaves. Application-layer firewalls scan and eliminate known malware attacks from the extranet before they reach a server or user's workstation, whereas intrusion prevention systems can identify and defeat advanced hacking techniques. All firewall rules have an associated security plan that describes the purpose and mitigating controls that are in place.

Layer 3: Strong Authentication
Following the recommendations of the National Institute of Standards and Technology, AIR requires a minimum of eight characters, using mixed cases plus a numeric or special character, for all passwords. User passwords are changed at least every 90 days, privileged access passwords more frequently.

Layer 4: Configuration, Patch Management
The importance of effective configuration and patch management of all devices on our network is fundamental, from border routers to data center servers and networked devices. We enforce the concept of adopting "least-user privilege" policies to reduce the risk of users introducing security flaws, and we continually monitor the network for vulnerabilities.

A.3. Application System Name/Title
The system as a whole is commonly referred to as the NHLBI HIC Inquiry and Inventory Management System, which includes WebSurveyor, the NHLBI Online Catalog, Integrated Publications site, Microsoft CRM, the Join the Health Information Network (HIN) opt-in e-mail list, and Microsoft Dynamics GP software.

A.4. Responsible Organizations
AIR is wholly responsible for the security, maintenance, and management of WebSurveyor, the NHLBI HIC Inquiry and Inventory Management System, and its related functions. Creation of and editorial changes to content are currently coordinated between the NHLBI and AIR under an existing contract.

A.5. Information Contact(s)

Principal Application Owner
Name: Lawrence Thomas
Title: Project Director
Address: American Institutes for Research Frederick Distribution Center
7315-A Grove Road
Frederick, MD 21704
Phone: (240) 629-3232
E-mail: lthomas@air.org

Manager With Expert Knowledge
Name: Larry Thomas
Title: Project Director
Address: American Institutes for Research
Frederick Distribution Center
7315-A Grove Road

Frederick, MD 21704
Phone: (240) 629-3232
E-mail: lthomas@air.org

A.6. Assignment of Security Responsibility

AIR Corporate-Level Security
Name: Robert McMahon
Title: AIR Chief Security Officer
Address: 1000 Thomas Jefferson Street
Washington, DC 20007
Phone: (202) 944-5260
E-mail: rmcmahon@air.org

Web Hosting Services Security
Name: Alex Padilla
Title: Director of Web Hosting Services
Address: 1000 Thomas Jefferson Street
Washington, DC 20007
Phone: (202) 403-5263
E-mail: apadilla@air.org

There are currently five distinct access roles associated with the NHLBI HIC Inquiry and Inventory Management System, which includes the WebSurveyor application to be used for the attached survey: network administrator, information specialist, software engineer, call center manager, and marketing manager.

Network Administrator. Five AIR staff members who make up our Web Hosting Services team can be defined as network administrators. This role is tasked with ensuring a stable and secure operating environment within which the NHLBI HIC Inquiry and Inventory Management System can function. This includes coordinating the day-to-day activities that ensure the system is online and highly available to the public and internal staff, as well as playing a pivotal role in establishing, and subsequently executing, a long-term vision that guards the security and reliable operation of the system. Day-to-day tasks associated with this role include:

- Managing backups of system files and data
- Installation of patches to ensure system security and stability
- Monitoring system log files for suspicious activity
- Assigning server-level access rights to users as needed
- Coordinating with vendors to replace and enhance system hardware as needed

Long-term tasks associated with this role include:

- Establishing guidelines for user passwords
- Providing direction and management of the long-term security methodologies used in AIR's production hosting environment

Due to the nature of this role, it is important that network administrators be physically located in close proximity to the system servers. Therefore, staff filling this position report to our Washington, DC, facility, where the system servers are physically located.

Information Specialist. Currently, seven AIR staff members are defined as information specialists. Users in this role work within a Windows client interface of Microsoft Dynamics GP, and a browser-based interface of Microsoft CRM—giving them access to the limited set of data that they need to perform their job and satisfy requests from the general public. These users do not have access to WebSurveyor or any of the data found therein. Tasks associated with the information specialist role that are relevant to the survey include answering any general technical questions regarding the survey.

Information specialists currently report to our Frederick, MD, facility, where our distribution facilities are located. They access the applications through a Terminal Services session over our internal corporate WAN to the GP server in Washington, DC, or via Web browsers installed on their local desktops connecting internally over our corporate WAN to the CRM server in our Washington, DC, facilities.

Software Engineer. Currently, two people fill the role of software engineer for the NHLBI HIC Inquiry and Inventory Management System. The software engineers are responsible for managing the database and the source code that runs the Online Catalog Web site and Integrated Publications system. The tasks associated with this role include:

- Responding to requests to provide custom programming and enhancements to the Online Catalog Web site or Integrated Publications system
- Maintaining the development environment for the Dynamics GP system
- Responding to requests from the call center to generate sales reports from Inventory and Sales data

These AIR staff currently reports to AIR's Washington, DC, facility. They access the NHLBI Online Catalog Web site internally over our corporate network via SFTP, Microsoft SQL Server Enterprise Manager, and Terminal Services.

Call Center Manager. The call center manager is responsible for managing information specialists and the processes that run the HIC call center. There is currently one person defined as the call center manager. As a part of his day-to-day work, he also works with the information specialists to resolve day-to-day issues in the call center and ensure enforcement of policies that require information specialists to log out of the computers when they are inactive and when they leave at the end of the work day. The call center manager will be responsible for training staff to answer any inquiries regarding the technical aspects of the survey.

Marketing Manager. The marketing manager helped design the survey and will be involved in the analysis of the results. She is responsible for promoting the Online Catalog Web site, the Integrated Publications site, and the HIN. Tasks associated with this role include:

- Analyzing Web usage logs
- Ensuring that the Online Catalog Web site receives high rankings in search engine placements
- Analyzing sales reports to determine which subject areas, target audiences, etc., are most highly in demand by the general public
- Devising a strategy for the placement and presentation, within the Online Catalog, of those NHLBI publications that have been identified as high-priority candidates for dissemination via the Web site
- Composing and mailing targeted e-mail campaigns to HIN members who have opted-in to receive e-mail and analyzing the effectiveness of those campaigns

This AIR staff member reports to our Silver Spring, MD, facility. The marketing manager uses the WebTrends Web Server Analysis to analyze Web server usage, and the NHLBI Intranet to generate targeted mailing lists for opt-in information dissemination activities.

A.7. Application System/Operational Status
The status of the NHLBI HIC Inquiry and Inventory Management System is **operational.**

A.8. General System Description/Purpose
Overview. The NHLBI HIC Inquiry and Inventory Management System includes the WebSurveyor application. The overall system is an e-commerce Web site and enterprise resource planning (ERP) system used to manage the inventory and public dissemination of NHLBI publications. It also includes the HIN, which serves as an important digital link between the NHLBI and the general public and health practitioners. The HIN enables the timely dissemination of targeted health information to those people who have identified themselves as having an interest in maintaining an ongoing relationship with the NHLBI, through the broadcast e-mail application Lyris.

Health Information Network. The HIN, built on the Lyris ListManager platform, is a Web-based e-mail subscription tool integrated with the Online Catalog database that enables the general public and health professionals to subscribe to receive health information and updates from the NHLBI. Subscribers sign up for membership online at http://emall.nhlbihin.net/hp2010/Default.asp and can further indicate their subject area interests, profession, and work settings. The Lyris ListManager database is hosted on AIR's secure networks in Washington, DC, and synchronization between the two systems is performed via a set of DTS jobs that transmit records internally over our Web Hosting Services network. The marketing manager then has password-secured access to the Lyris database that enables the generation of mailing lists that contain addresses for HIN members who are interested in receiving NHLBI e-mails. Moreover, the marketing manager is able to created targeted lists based on interest areas, professions, etc. The HIN, in its current incarnation, has grown to account for more than 100,000 active members who have elected to receive e-mail from the NHLBI.

A.9. Application System/Environment

AIR's NHLBI HIC Inquiry and Inventory Management System is based on a client-server architecture and includes an e-commerce Web site that runs over an SSL-encrypted communication channel as information specialists interact with NHLBI's Web-based services via their personal Web browsers.

Server Architecture. The server architecture comprises multiple Windows 2003 servers located in AIR's Washington, DC, facility. The servers that make up this multiserver architecture can be mapped physically and logically into two functional tasks as follows:

- **Back Office.** Management of the back office master data accessed by warehouse staff via Dynamics GP clients and the NHLBI Intranet.
- **Front Office.** Management of the Web site by Web Hosting Services staff over our internal network and use of the Web site by the general public via their personal Web browsers.

The back office server component is comprised of one server, and the front office server component is comprised of the other servers in this multiserver architecture. Key hardware and software configurations that enable these systems to satisfy the business requirements of this project follow.

The physical and logical separation of these two processes in the multiserver architecture renders a system that is more highly available than one where the front office and back office are married into one physical system. For example, when maintenance or a reboot must be executed on the back office system, the NHLBI Online Catalog Web site and the Integrated Publications site can continue to function and accept orders from the public. When the back office system is brought back online, it uses Dynamics GP BDX services to automatically synchronize any orders that were received into the front office while it was down.

This multiserver architecture is physically located in our Washington, DC, facility, and isolated on a dedicated internal subnet separated from both the internal AIR network commonly used by AIR staff and the public Internet by enterprise-grade firewall managed by the AIR Web Hosting Services team. In addition to the firewall, Web Hosting Services has deployed an intrusion prevention system appliance that can employ granular security policies commensurate with the level of risk on a per host basis. For security purposes, only the Web server itself is accessible from the Internet, and even then, solely over ports 80 and 443 for HTTP and SSL-encrypted HTTP, respectively. The front office database and the back office Dynamics GP database servers are not Internet-accessible and, furthermore, are accessible strictly from within the internal AIR network only to those users whose roles require that they be expressly granted access to these systems. Internal access to the servers may take the form of SFTP to the Web server, Terminal Services to any servers, directly via the local console, or via an installed eEnterprise client. Authorized internal users are able to access only those servers to which they need access, and only via the methods that are applicable to their specific roles.

A.10. Application System Interconnection/Information Sharing

Some information from the NHLBI Dynamics GP database is accessed by the Lyris database and the Microsoft CRM system, and by the NHLBI Intranet. The NHLBI Intranet is physically

located at AIR's Silver Spring facility and is able to connect to the data that is needed in the NHLBI HIC Inquiry and Inventory Management System. The NHLBI Intranet accesses the GP data for the following purposes:

- To render a count of registered Web site users over time
- To provide for the approval of reader reviews from the Online Catalog

Data that are transmitted to the NHLBI Intranet server are also stored in a database at AIR's Washington, DC, facility. This database server is inaccessible to the general public.

The Lyris database connects to the Dynamics GP database for the purposes of creating mailing lists so that the NHLBI can run effective e-marketing campaigns by sending broadcast opt-in e-mails to its constituency. This database is also hosted in our Washington, DC, facility and managed by the same Web Hosting Services staff who administer the Dynamics GP hardware.

The Microsoft CRM system connects to the Dynamics GP database for the purposes of synchronizing orders and customer information. If an order is placed via the Online Catalog, the status of the order can be looked up in the Microsoft CRM system. This server is also hosted in our Washington, DC, facility and managed by the same Web Hosting Services staff who manage the Dynamics GP and Lyris systems.

A.11. Applicable Laws or Regulations Affecting the Application

- Federal Information Security Management Act (FISMA)
- Office of Management and Budget (OMB) Circular A-130
- Privacy Act of 1974

A.12. Information Sensitivity and Criticality Assessment

Due to the nature of the NHLBI HIC Inquiry and Inventory Management System—receiving and fulfilling requests for health information from the public, survey results through WebSurveyor, etc.—it must provide for the secure retention and management of a myriad of sensitive data elements. The system is currently responsible for guarding information such as:

- Personal address and e-mail information
- Survey results
- User demographics (interests, occupations, and work setting)
- Inventory information

Table A. Application/System Protection Requirements

Application/ System Protection Requirements	High	Medium	Low
Confidentiality	• Personal addresses • Survey results • Order history • User demographics		• Inventory
Integrity	• Personal addresses • Order history • User demographics • Inventory		
Availability	• Personal addresses • Order history • Inventory	• User demographics	

Were the above referenced information compromised and released to an ill-minded user, it could cause degradation in the valued trust that the general public currently has placed in the NHLBI. The NHLBI has committed to all those who participate in the survey that their responses will be strictly confidential, secure, and not linked in any way to personal and/or identifying information. It is therefore absolutely vital to the success of this information dissemination project as well as to protecting the public trust in the NHLBI and the NIH that this information continue to remain completely secured and inaccessible to all but those business processes and roles that require it.

B. Management Controls

B.1. Risk Assessment and Management

Potential vulnerabilities in the NHLBI Online Catalog and Integrated Publications sites are continually scanned with monitoring tools managed by our Web Hosting Services team. NIH has performed periodic scans of the system and found the system to pass. This tool scans systems for vulnerabilities and receives automatic updates of these potential threats to better manage the environment at a day-to-day operational level.

As part of the AIR Information Security Program, security testers perform security assessments and audits of all critical systems. AIR security testers understand that no one tool addresses all security issues; therefore, assessments will involve the use of multiple commercial and open-source tools in order to provide adequate coverage of security vulnerabilities. The use of all tools is tightly controlled to ensure that testing does not negatively impact operations.

As a methodology, AIR uses a combination of manual and automated techniques to assess management, operational, and technical controls. To assist with automated testing, AIR has invested in the capability to perform in-depth, scalable, and repeatable Web application testing of Web Hosting Services-hosted Web application servers. Internal AIR security assessments will generally involve both red team testing (e.g., having only the knowledge a

hacker would have) and cooperative testing using ”valid” user credentials, internal network designs, or other forms of “inside” knowledge.

Web applications assessments, at a minimum, detect the following kinds of vulnerabilities and exposures:

- Authentication and authorization
- Buffer overflows
- Malicious file execution
- Code injection (e.g., SQL, XPath, LDAP, MX, Shell Command)
- Information leakage and improper error handling
- Cross-site scripting and cross-site request forgery
- Insecure communications

Through these tools, AIR is continuing to improve the security practices and mindset used during our development cycles and operational activities.

B.2. Review of Security Controls

There has not yet been an independent risk assessment review of the NHLBI HIC Inquiry and Inventory Management System performed by a third party outside of NIH and AIR.

B.3. Rules of Behavior

All AIR staff who have access to the system are expected to behave within the bounds of reasonable access behaviors, as published in the AIR employee guide and widely disseminated throughout the company on the AIR Intranet. These defined rules of appropriate behavior, as presented to AIR staff, include:

- Personal or private data should not be stored on the network.
- All employees will use the network and e-mail in a manner that is responsible, that does not cause harm, and that does not conflict with the policies of AIR.
- Under no circumstances should an employee download or copy any computer programs available on the Internet without prior approval from the IT department.
- If software is needed to perform work assignments, requests for such software should be directed to the IT department, which is responsible for reviewing purchase requests and testing nonstandard software before it is installed.
- Do not open suspicious messages or attachments, and do not route virus warning messages to other AIR employees.
- Sharing of one’s personal password to other users is strictly prohibited.
- AIR prohibits interference with the intended use of its computers and information systems. Examples include knowingly introducing a computer virus, flooding the network with unauthorized traffic, or altering or compromising the integrity of the information resource.

Employees are further advised that they are held personally and individually responsible for all actions performed using the AIR network and its related systems. Violations of any guideline are subject to immediate disciplinary action to include suspension of employment or discharge, in addition to possible criminal and civil penalties. If necessary, the company will advise appropriate officials of any illegal activity.

B.4. Planning for Security in the Life Cycle

Initiation. As the project plan for the NHLBI HIC Inquiry and Inventory Management System was created, AIR Web Hosting Services staff were brought in to coordinate the design of a secure system.

Implementation. As the system was implemented, it was stress tested, and availability and security monitoring tools put into place.

Operation/Maintenance. The system, currently in its operation and maintenance state, is continually scrutinized by AIR security tools and procedure. Upgrades and patches to the system are performed at regular intervals and on an as-needed basis by the Web Hosting Services team. Moreover, the automated monitoring and security assessment tools put into place in the implementation phase continue to be supported. New tools are added as business requirements demand.

B.5. Authorization To Process

The NHLBI Online Catalog/GP eEnterprise system was given authorization to process data from Glen Bennett and Chris Olaes via e-mail on April 11, 2001.

C. Operational Controls

C.1. Personnel Security

All new AIR employees undergo a criminal background check as well as verification of employment and an educational background check. Credit reports are obtained for staff in high-risk positions (e.g., finance-related jobs). All personnel working on Federal Agency contracts are subject to personnel suitability screening in accordance with contract requirements.

AIR implements procedures that ensure consultants, contractors, and temporary workers sign confidentiality and nondisclosure agreements before being granted access to any AIR information systems or proprietary information in accordance with published guidance.

The Human Resources (HR) department will notify Web Hosting Services when employees are terminated to ensure that access to information systems is revoked in an expedient manner. System access for voluntarily separated personnel will be terminated no later than the close of the employee's last business day unless an exception is approved by both HR and the employee's program director. This applies to password, account user IDs, e-mail use, and all other access methods.

User access is restricted to the minimum necessary to perform a particular job. For example, users working as information specialists have no access to the servers themselves and may only access the Dynamics GP data through the eEnterprise client and the functionality that it provides.

Moreover, within the Dynamics GP client, their access is limited only to those tasks that they must be able to perform. They cannot create new users or modify item descriptions or price schedules, etc. When a new user arrives and requires an account to access the system, the appropriate personnel are notified of this need by the new employee's manager. If the new user is an information specialist in need of an account, then the call center manager sends an e-mail to the software engineer requesting the creation of a new Dynamics GP or CRM account. If a new software engineer or call center manager needs access to the system, an e-mail is sent from the managing project specialist identified in section A.4 to the network administrator to grant SFTP or terminal services access to the server itself. If an employee leaves the company or changes their job function such that he or she no longer needs access or can function with reduced access to the system, a similar process is followed to disable his or her access.

The roles and duties mentioned in section A that comprise the business processes, administration, and workflow of the NHLBI HIC Inquiry and Inventory Management System are distributed across a range of staff. No individual staff member serves concurrently in more than one role.

C.2. Physical and Environmental Protection

The NHLBI HIC Inquiry and Inventory Management System server system is physically protected behind three strictly controlled access points in AIR's Washington, DC, facility. In order to gain physical access to the servers, an individual must first gain admittance to:

- AIR's corporate offices via an electronic key card
- A floor to which access is also control by an electronic key card
- The server room itself, controlled by a combination lock and monitored by video cameras

The building in which the servers are located is protected by standard fire safety equipment—sprinklers, fire extinguishers, fire alarms—and is situated 0.8 miles from the nearest fire station. The server room is supported by UPS and backup generators in the event of a failure to the electrical utilities servicing the facility.

AIR's Silver Spring and Frederick, MD, facilities, which host the handful of client machines, are each physically protected by electronic key card access. Moreover, access to the offices in which the client machines are located is restricted by a crew that locks all of the office doors at the end of each business day. Staff are also required to logout and power their desktop computers off before leaving at the end of each work day.

C.3. Production Input/Output Controls

Information specialists serve as an important conduit to help for the general public. Problems and complaints with the NHLBI Online Catalog that are e-mailed to the information specialists are stored in the Microsoft CRM system. The Microsoft CRM system is able to track the activities and changes to the system and report on them at regular intervals. If a change occurs to an inquiry in CRM, or to an order in GP, the username and date of the change are recorded in the database for future reference. The Online Catalog Web site includes a privacy statement establishing the fundamental guidelines with which trusted user information is protected and not shared with third parties. When backup media are reused, the standard procedure is to overwrite the media with the new backup dataset. Access via the Web site to order history information for

users is guarded by requiring the keying of a username and password. Recognizing the importance of the public trust placed in the NHLBI, when an Internet order is placed, any attempt made by an Internet user to examine the order history of an account not their own is stopped, a warning is issued, the event is logged into the GP database, and the software engineer is immediately notified of the event via e-mail.

C.4. Contingency Planning

Backups. All servers are currently backed up on daily, weekly, and monthly schedules. Daily and weekly backups are stored onsite in a locked safe that is further physically secured behind three strictly controlled access points. Monthly backups are stored offsite at Iron Mountain, an industry leader in offsite data storage and protection. Monthly backups are stored at Iron Mountain in secure vaults. These backups are shipped to Iron Mountain in a locked case via an Iron Mountain courier. Daily backups are maintained for 30 days and then the media are overwritten. Monthly backups are retained for 90 days before the media are overwritten. Databases and the programming code that allows the NHLBI Online Catalog Web site to function are currently included in the backup routines. Since the system is designed as a client-server architecture, with no data stored on client machines, backups of individual client machines are unnecessary.

In the event of a system failure, the network administrator will pull the most recent database and Web site backups, reinstall the operating systems, and subsequently restore any databases or code that may have been lost during a the failure. With a backup routine that includes daily backups, in a worst case scenario, any restored code and data will be assured of being no more than 24 hours old.

C.5. Application/System Hardware and Software Maintenance Controls

Maintenance. The only individual(s) authorized to perform hardware and software maintenance and repair activities in the NHLBI HIC Inquiry and Inventory Management System are those who perform the network administrator role. This currently amounts to the Web Hosting Services team, a set of staff whose sole purpose is to ensure the security and reliability of our production hosting environments. Moreover, network administrators are restricted from taking down the system without the express permission of the managing project specialist, who in turn must inform the client of the possibility of impending downtime and the causes thereof.

In the event that a piece of hardware must be serviced offsite, any data storage media (hard disk, compact disks, etc.) are removed from the unit and remain at AIR facilities. In the event that remote access must be granted to provide support to the system, a knowledgeable AIR employee must at all times be able to view the remote session and speak in real time over the telephone with the support personnel. Over the most recent contract period, there has been only one occurrence for such an event. The support representative was an authorized technical support employee of Microsoft Dynamics GP functioning under an existing support contract between AIR and Microsoft Dynamics. The remote session was wholly under the supervision of the software engineer.

Licensing. All software and operating systems on the multiserver architecture have been legally licensed to run per the licensing agreements invoked by each respective software vendor. It is AIR policy that the pirating of illegal software and desktop installation of nonstandard,

unapproved software is strictly prohibited. Moreover, AIR maintains a list of the standard software employees need to perform their work functions. This list is made readily available to all AIR staff via the AIR Intranet and all AIR staff members are expected to comply with this list in whole.

Change Control. There are four types of potential changes to WebSurveyor and its associated applications:

1. Upgrades
2. Changes
3. Routine installation of system patches

Upgrades. When the WebSurveyor application is slated to receive an upgrade, a comprehensive impact analysis is performed by:

- A comprehensive review of upgrade documentation
- Consultation with developer technical support personnel
- Installation and upgrade on a test bed so that the process may be given a dry run to target and identify resolutions to any potential issues in the upgrade process
- Intensive coordination between the network administrator, call center manager, software engineer, and managing project specialist roles identified in section A.5, as well as other project management and corporate IT staff who need to be consulted

Routine Installation of System Patches. As needed or required, the network administrator performs routine maintenance in the NHLBI HIC Inquiry and Inventory Management System. This includes the installation of any vendor patches that have been released. Prior to this maintenance, the network administrator creates a disk image of the existing servers. In the event of a system failure during the installation of these patches, the network administrator is able to restore any failed systems back to their original state using the disk image that was created immediately prior to the maintenance routine.

C.6. Data Integrity/Validation Controls

All of the servers in the NHLBI HIC Inquiry and Inventory Management System run Symantec Anti-Virus Server software. The virus signature files on each server are automatically updated on a daily basis. Nessus is used to automate the testing and discovery of known security problems before they can be leveraged by potential intruders. The NHLBI HIC Inquiry and Inventory Management System currently includes numerous layers to detect system failure and intrusion activity. Internal to the AIR network, a system monitoring tool called Servers Alive checks to see whether the systems are available at regular intervals. In the event that any of the servers is not available, a member of the Web Hosting Services team is paged and responds to bring the server(s) back online. An external monitoring service provided by dotcom-monitor.com is used to monitor the Web server from an external source. This monitoring service also checks the Web server every 15 minutes and, in the event of system failure or alteration of content that may be indicative of a system compromise, the network administrator is notified and responds in suit. Moreover, the Web Hosting Services team has automated tools for reviewing the system log files and notifying staff of suspicious activities.

C.7. Documentation

Documentation is available for the NHLBI HIC Inquiry and Inventory Management System. This includes:

- Administrator guides
- Network diagrams
- Training documents for information specialists
- Contingency plans

The documentation for the system is available on the AIR network file system.

C.8. Security Awareness and Training

The network administrator is sent to security training, including the Global Knowledge security seminars, several times per year. Information specialists have been trained by a Certified GP administrator in their daily tasks. Moreover, AIR maintains a support contract with Microsoft GP Business Solutions that allows us to receive unlimited support regarding security issues and questions that may arise.

C.9. Incident Response Capability

If a system has been compromised, the network administrator executes the following procedure:

- An immediate record is taken of the running services, open ports, and the processes that are communicating with them
- Removes all hard disks to ensure evidence preservation
- Reinstalls and rebuilds the systems

The software engineer then performs a detailed review of the data and programming code to ensure their integrity before the system is brought back online. Any log files from the old system (security, system, Web, and applications logs), as well as firewall log files are then analyzed for events that may be indicative of intrusion or system failure. When a system failure occurs, the network administrator is notified via e-mail and pager of the event. The network administrator also has readily available the home and mobile phone numbers of critical staff such as the software engineer and managing project specialist in the event that they need to be involved or advised in recovering the system to its operational state.

Whenever an incident involving system failure or compromise occurs, the managing project specialist notifies the NHLBI of the event.

D. Technical Controls

D.1. Identification and Authentication

The system uses several access control methodologies—server, SQL Server, and SFTP.

Server. Access to the servers themselves is controlled at the operating system level, and those users accessing the servers directly must have a Windows 2003 user account set up by the

network administrator. Server access passwords must adhere to a combination of various types of characters and minimum length and must be changed every 30 days. Users are allowed a small number of invalid access attempts, after which their accounts are locked out for 30 minutes. Moreover, invalid access attempts are also logged in the server security logs. If users forget their password, the only way that they can gain access to the system is by contacting the network administrator, who in turn must reset their Windows password. If a user's password expires, he or she is subsequently prompted to create a new password at the next logon attempt. There are no methods for bypassing the logon prompt. Any user wishing to enter the system at this level must enter a password in order to gain access.

SQL Server. Users who access the database directly must do so using SQL Server authentication. Access to the database is restricted to being accessed solely from within the AIR network, not over the Internet. Password policy is currently limited to the password management policies native to SQL Server authentication. As such, passwords are not automatically forced to expire. However, direct SQL Server access is a strictly guarded privilege that is afforded only when required—currently this would be the network administrator and the software engineer.

SFTP. SFTP access to the servers is granted to those roles that must be able to upload ASP files and images to the Web server. This is currently limited to the software engineer role. SFTP access is regulated by Windows 2003 and IIS; therefore the password characteristics and lockout policies are identical to those of the server access method described above. Since this method uses SFTP, the passwords do traverse the network in plain text. However, SFTP access to the Web server is only possible from within and over the AIR corporate network. Therefore, these system-level passwords do not traverse the public Internet at any point during the authentication process.

For none of these authentication methods is there a policy in place that provides for bypassing standard login policies.

D.2. Logical Access Controls

The systems are able to restrict users from accessing those functions and datasets to which they need not have access by providing a security framework that supplies predefined user roles. For example, information specialists are restricted to accessing and modifying only data required by their role. At the server level, the network administrator actively uses the standard Windows 2003 security architecture to prevent unauthorized access of internal users to those system resources and functions that they do not need to perform their jobs.

Access rights to the servers and SQL Server are granted by the network administrator after receiving an account creation request from a qualified manager. Access rights to the system via the e-client are granted by the software engineer after receiving a request from the call center manager. There are currently no restrictions on qualified personnel accessing the system after normal working hours, however, the system does provide for such a policy to be implemented if a business need arose. Users logged directly into the servers are automatically logged out after 30 minutes of inactivity. Users logged into the client are logged out after an inactivity period of 1 hour. All staff in the information center are required to close their sessions at the end of each business day. Moreover, AIR has designed an internal tool that enables the software engineer or call center manager to remotely log out any users who are still logged into the system.

D.3. Public Access Controls

Members of the public access WebSurveyor through their Web browsers. Respondents login with their e-mail address and a password of their own choosing.

WebSurveyor and Lyris will be loaded with the e-mail addresses of users invited to participate in the survey. Once a user has logged on to the WebSurveyor page for the survey, WebSurveyor and Lyris will note same in the application database. Users will be able to take a break by logging off and returning to complete their survey; or more likely, complete the survey on their first access. Once a user has submitted his or her responses and closed out the survey, the WebSurveyor and Lyris applications will close out that record and block any attempt to log on to the Survey by repeat users.

If a user forgets his or her password, he or she may use a "forgot password" tool on the Web site that will e-mail it to the e-mail address that the user has registered with his or her account. When users terminate their browser sessions, they are automatically logged out of WebSurveyor and must log back in if they return to view any personal information.

On the Web server, users are restricted to viewing only their own responses and not that of other users. Attempts to view the information other Web users are strictly prohibited, logged, and a warning message rendered in the offending users browser. The WebSurveyor survey is designed to be available to the public over the Internet on a 24/7 basis for the duration of the survey, with periodic monthly maintenance windows that last up to several hours and are performed on a weekend and after hours.

D.4. Audit Trails

The NHLBI HIC Inquiry and Inventory Management System is supported by a rich set of auditing tools and processes that are constantly evolving and improving to ensure long term system security and incident review.

The servers themselves provide for auditing of many user actions through the native Windows 2003 logs. The Dynamics GP platform and CRM application tracks system changes within at the application level, recording changes that are made, when they are made, and the user who made the change. SFTP access is logged in log files for review. HTTP access is logged in the IIS WWW service logs. The network administrator has access to the server system logs, and they are scanned by automated tools. The software engineer has access to the audit logs. HTTP access is generally reviewed in an aggregate form unless suspicious patterns that may be indicative of abuse appear.