

**National Cancer Institute (NCI)**

**caArray**

Questionnaire

February 1, 2011

# Introduction

The Federal Information Security Management Act (FISMA) of 2002 – contained within the E-Government Act of 2002 (Public Law 107-347) –places requirements on Government Agencies and supporting organizations, with the goal of improving security of federal information and information systems. FISMA requires each federal agency to provide information security protections commensurate with the risk and magnitude of harm that may result from unauthorized access, use, disclosure, modification, or destruction of its information and information systems. Additionally, each Federal agency must report to Congress annually (by the first of March) on the adequacy and effectiveness of information security policies, procedures, and practices to support FISMA compliance.

Security Authorization, also known as Certification and Accreditation (C&A), is an important activity that supports an agency’s risk management capability and is an integral part of the IT security program. Furthermore, it serves an initial first step towards becoming FISMA compliant. The National Institute of Standards and Technology (NIST) develops and issues standards, guidelines, and other publications to assist federal agencies in implementing FISMA and in managing programs that protect their information and information systems. This guidance and recommendations are issued as part of the NIST Special Publication (SP) 800-series. The schedule for complying to FISMA and the NIST guidelines for legacy systems, is within one year of the publication date. For systems under development, agencies are expected to comply with NIST and FISMA guidelines immediately upon deployment.

The Office of the CIO (OCIO) is in process of ensuring that all major and minor applications (current and under development) supporting NCI meet basic security standards in keeping with latest Federal laws, directives, and guidelines. This questionnaire is designed to identify key security components, controls, and artifacts that demonstrate an organization’s FISMA compliance. The OCIO will use information collected as part of this exercise to 1) obtain a basic understanding of each organization’s current security posture, and 2) identify deficiencies before granting each system a formal Authority To Operate (ATO).

**Steps and Instructions:**

Please complete the following questionnaire to assist the NCI Security Team in completing the upcoming C&A of this system. Information collected from this questionnaire will assist the C&A Team in completing multiple components of the C&A package and properly define the accreditation boundary. Additionally, your assistance in completing this will help limit our data collection process by collecting information once and applying to several key C&A documents.

Please note the following instructions for completing this exercise:

* The following questionnaire should be completed by each organization’s IT Security Officer or System Owner and returned to NCI − along with any supporting security documentation − within three weeks of receiving this notice.
* Please complete and return this questionnaire in electronic format via email.

**Delivery Information:**

Upon completion, please send the Security Authorization questionnaire and supporting security documentation to:

Craig Hayn

Security Contractor

National Cancer Institute (NCI)

6116 Executive Blvd

Suite 501

Rockville, MD 20852

301.402.4016

haync@mail.nih.gov

# System Background Information

a) The first step towards FISMA compliance is to determine what constitutes the “information system” in question. Please complete the table below with the applicable organization/study and system information.

|  |  |
| --- | --- |
| **System Information** | |
| Category | System Details |
| Organization (NCI/Center/Office/Division): | NCI/CBIIT |
| Information System Name: | caArray |
| Information System Type\* (Major Application or Minor Application): | Minor Application (NCI LAN child application) |
| Status of System (Development, Production, or Modification): | Production |
| Planned Deployment Date: | <INSERT DATE> |

|  |  |  |
| --- | --- | --- |
| **Key Security Roles and Responsibilities** | | |
| System User\* | Name | Contact Information (Phone or Email) |
| Information System Owner: | Juli Klemm | klemmj@mail.nih.gov  <INSERT CONTACT NUMBER> |
| Project Manager | Makiko Duncan | [duncanmk@mail.nih.gov](mailto:duncanmk@mail.nih.gov)  <INSERT CONTACT NUMBER> |
| Information System Security Officer: | Bruce Woodcock | [woodcockb@mail.nih.gov](mailto:woodcockb@mail.nih.gov)  301-594-0686 |
| System Administrator: | <INSERT NAME> | <INSERT CONTACT INFORMATION> |
| Database Administrator: | <INSERT NAME> | <INSERT CONTACT INFORMATION> |
| User Representative: | <INSERT NAME> | <INSERT CONTACT INFORMATION> |
| Development Lead: | <INSERT NAME> | <INSERT CONTACT INFORMATION> |
| IT Security Officer: | <INSERT NAME> | <INSERT CONTACT INFORMATION> |
| Other Key Personnel: | <INSERT NAME> | <INSERT CONTACT INFORMATION> |

\* Please refer to the Glossary and Appendix A for formal definitions of application types and key personnel.

b) Complete the table below with the business purpose and scope of the information system. Please include a list of system users (stakeholders) and data types that will be maintained and processed within the system.

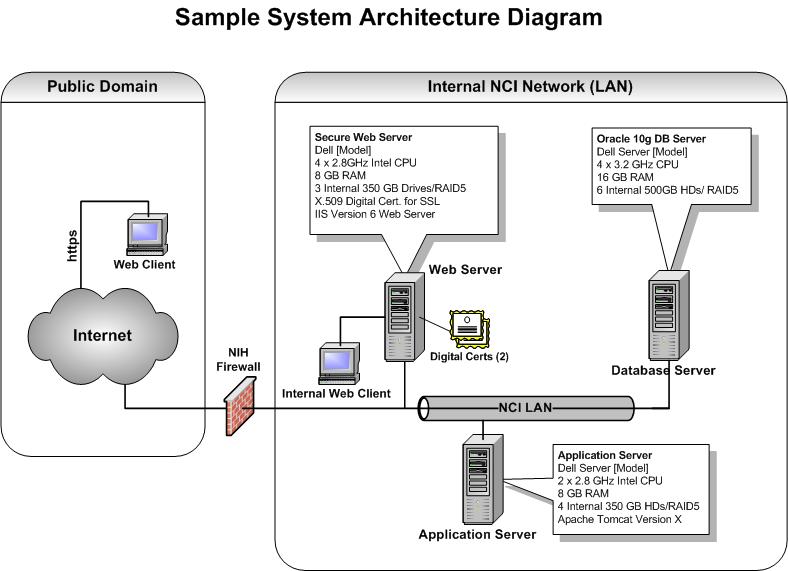
|  |
| --- |
| **System Purpose, Users, and Data Types** |
| Example: The XYZ Database (XYZ SYSTEM) is a central storage database hosting genetic code research information used by genetic medicine interns The XYZ SYSTEM stores Privacy Act information (SSN, full name, home address, and telephone numbers) of all the research subjects, which are male and female between the ages of 12 through 40. The XYZ SYSTEM contains approximately 2,600 records.  There are approximately 800 internal users (genetic medicine interns), and 35 external users (John Hopkins University research fellows) and 4 privileged users (1 system administrator for the web server, 2 database administrators for the oracle database). The data type processed and stored by this database is the XYZ Research Information Type as defined by NIST 800-60.  <INSERT BUSINESS PURPOSE> |

c) Complete the table below with the technical system description and scope (system boundaries). Please provide a description of the systems current state (design, development, production, modification, or disposal). Additionally, list all interconnections with other major applications and the general support system (i.e., Local Area Network). Please do not include network services (e.g., routers, switches, firewalls, etc…) unless they are dedicated to your system.

|  |
| --- |
| **Technical System Description** |
| Example: The XYZ System is a central storage database hosting genetic code research information used by genetic medicine interns The XYZ SYSTEM stores Privacy Act information (SSN, full name, home address, and telephone numbers) of all the research subjects, which are male and female between the ages of 12 through 40.  The XYZ SYSTEM consists of three components, and the three components represent the entire system boundary:   1. Web Server – XYZ SYSTEMWWW4 2. Report Generation Server - XYZ SYSTEMSQLRPT 3. XYZ SYSTEM Database Server – XYZ SYSTEMDB   The Web Server is used to enter data via the web using an HTML and Oracle forms based website found at [www.XYZ Systemdb.com](http://www.grddb.com/). The site is also used to generate reports which allow a user to interface with the XYZ SYSTEM DB indirectly via the XYZ SYSTEMSQLRPT server and obtain timely genetic test research information.  The XYZ SYSTEM DB is not directly connected with any users in order to prevent allowing any user direct access to its data and records. This is a mechanism to prevent direct attacks against the database.  The XYZ SYSTEM is considered a major or minor application and is in the production phase of its lifecycle. The XYZ SYSTEM interconnects with the following systems:   1. Medical Tissue Center (MTC) – Internal to NCI CBIIT 2. Medical Research Center (MRC) 3. Data Warehouse Database (DWD)   All systems that the XYZ SYSTEM DB interfaces with are external to the XYZ SYSTEM DB but not external to the organization.  <INSERT TECHNICAL DESCRIPTION> |

d) Please insert the latest system diagram that displays the major system components, interconnections, and end users.

Sample Diagram below:



<INSERT DIAGRAM>

e) If known, please provide a complete system inventory that includes the exact number and types of components (vendor name and product number), and software (name, version) and operating system (type and version).

| **Component Name/Server Name** | **Hardware**  **Manufacturer**  **(Name/Version)** | **Software (Name/Version)** | **Hosting Facility** | **Primary IT Function** |
| --- | --- | --- | --- | --- |
| cbvapp-p1001 Server | Example: VMware Virtual Machine  <INSERT HARDWARE> | Example:  Windows 2003 Server Standard 32-bit  .NET environment  <INSERT SOFTWARE> | Example:  Bldg X, Room X  <INSERT BUILDING> | Example:  APPLICATION SERVER  <INSERT FUNCTION> |
| cbws-p1001 Server | Example: HP DL380 G4  <INSERT HARDWARE> | Example: Windows Server 2003  <INSERT SOFTWARE> | Bldg X  <INSERT BUILDING> | XYZ Database Report Server  <INSERT FUNCTION> |
| XYZDB  <INSERT COMPONENT NAME> | Example: HP DL380 G4  <INSERT HARDWARE> | Example: Windows Server 2003, SQL 2003 <INSERT SOFTWARE> | Bldg X  <INSERT BUILDING> | XYZ Database Server  <INSERT FUNCTION> |

f) Please provide information on where the system is hosted (NCI CBIIT, NIH CIT, hosted externally at Iron Mountain, etc…).

g) Please list the system’s development environment (.NET, Cold Fusion, Php, etc…).

h) Please include web platform (IIS, Apache, Apache Tomcat, etc…).

i) Please include site URL(s).

j) Does this application have any of the following documentation (if so, please provide separately with completed questionnaire):

If not, are they covered by other organizational documents and procedures?

|  |  |  |
| --- | --- | --- |
| **Document** | **Yes/No** | **Inherited?** |
| Memorandum of understanding (MOU) or Interconnection Security Agreement (ISA) |  |  |
| Service Level Agreement (SLA) |  | X - CBIIT |
| Disaster Recovery Plan |  |  |
| Incident Response Plan |  | X – CBIIT |
| Contingency Plan  Disaster Recovery Plan/Steps |  |  |
| Configuration Management Plan (for caArray, not for infrastructure) |  |  |
| SDLC Development Process |  |  |
| User Guide (vendor doc and training doc) |  |  |
| Administrator’s Guide (Vendor doc) |  |  |
| Account Management Guide |  |  |
| Audit Log Management Standard Operating Procedures (SOP) |  |  |
| Vendor documentation |  |  |
| Rules of Behavior |  | X-Inherit from NIH |
| Acquisition contracts SOP |  |  |
| Site License Documentation |  |  |
| Design Documentation |  |  |
| Records of Security Alerts and Advisories |  |  |

# References

The following publications are guidelines to conducting information system C&A’s and obtaining compliance with FISMA.

* FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems;*
* FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems;*
* NIST Special Publication 800-18, *Revision 1,* *Guide for Developing Security Plans for Federal Information Systems;*
* NIST Special Publication 800-30, *Revision 1, Guide for Conducting Risk Assessments;*
* NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems;*
* NIST Special Publication 800-37, *Revision 1,* *Guide for the Security Certification and Accreditation of Federal Information Systems;*
* NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems;*
* NIST Special Publication 800-53A, *Revision 1,* *Guide for Assessing the Security Controls in Federal Information Systems;*
* NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System;*
* NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories;*
* NIST Special Publication 800-63-1, *Draft Electronic Authentication Guideline;*
* NIST Special Publication 800-70*, Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers; and*
* NIST Special Publication 800-100, *Information Security Handbook, A Guide for Managers*.

<http://csrc.nist.gov/publications/nistpubs/>

# GLOSSARY

**Account Management Guide:** This document establishes the password policy and standards for the administration of accounts that facilitate access or changes to a system’s information systems and data. Supplying account information to approved end users will grant specific role based access to some set of services and resources within a system. This document establishes guidelines for issuing accounts, creating password values, and managing accounts throughout the account life cycle.

**Accreditation:** The formal declaration by the DAA that the system is approved to operate using a prescribed set of safeguards and should be strongly based on the residual risks identified during certification.

**Acquisition Contracts:** These comprehensive documents defines the efforts required to acquire resources, ensures coordination of all human and organizational resources involved in fulfilling the organization's needs in a timely manner and at a reasonable cost, and should take into account the security requirements of the system as part of the criteria for acquiring a resource.

**Administrator’s Guide**: This document provides direction on how to use and access a system from the perspective of the administrator. Often, it will include installation and vendor recommended baseline configuration instructions. If a system is an upgrade, often it will highlight the differences between the upgrade and the previous version.

**Audit Log Management Standard Operating Procedures:** This document establishes a system’s logging and auditing policy and procedures, identifies staff roles and responsibilities in support of audit and accountability procedures. In addition, the document addresses: (i) the creation, protection, and retention of information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) how the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

**Availability:** Ensuring reliability and timely access to data and resources to authorized individuals.

**Certification:** The comprehensive assessment of technical and non-technical security features and other safeguards associated with the use and environment of a system to establish whether the system meets a set of specified security requirements.

**Certifying Authority:** This individual assumes the role of an independent technical liaison for all stakeholders involved in the C&A process and is an objective third party, independent of the system developers. The Certifying Officer provides a comprehensive evaluation of the system, including technical and non-technical controls, to determine if the system is configured with the proper security controls in place.

**Confidentiality:** Ensuring the prevention of unauthorized disclosure.

**Configuration Management Plan:** A plan that describes the management controls involved in all changes and updates made to a system that affects security. The plan includes all documentation supporting these changes and updates. This plan is maintained throughout the C&A process and updated according to system development lifecycle (SDLC) activities.

**Contingency Plan:** Preventive measures established to assist an organization in their ability to quickly and cost effectively recover critical IT resources.

**Continuity of Support:** Preventative measures for protecting the IT systems as well as procedures for restoring any system disruption.

**Design Documentation:** This document captures design decisions and solutions, explains the rationale and implications of the design, and presents system specifications.

**Designated Approving Authority:** This individual is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals.

**Disaster Recovery Plan:** A plan that identifies recovery procedures in the event of natural or man-made disasters or catastrophes affecting the availability of the system. This plan is tested annually to ensure the continued effectiveness and adequacy of the plan.

**General Support System:** A collection of interconnected information resources under the control of a single authority and security policy, including personnel and physical security, which shares common functionality. Provides standard information security capabilities, such as boundary defense, incident detection and response, and key management, and also delivers common applications, such as office automation and electronic mail.

**Information Sensitivity:** The formal process of identifying each system in terms of its confidentiality, integrity, and availability.

**Integrity:** Ensuring the accuracy and reliability of the information in the system and prevention of any unauthorized modification.

**Incident Response Plan:** The plan that directs how computer incidents are to be handled and identifies the entities who need to respond to the incidents and the entities’ roles and responsibilities.

**Interconnection Security Agreement:** This document establishes procedures for mutual cooperation and coordination between two systems regarding the development, management, operation, and security of a connection between the systems. Additionally, the document is intended to minimize security risks and ensure the confidentiality, integrity, and availability (CIA) of the information of one system as well as the information that is owned by the external organization that has a network interconnection with the system. This ensures the adequate security of the information being accessed and provides that all network access satisfies the mission requirements of both systems.

**Major Application:** A system that performs a clearly defined function for which there are readily identifiable security considerations and needs (e.g., an electronic funds transfer system or an air traffic control system).

**Memorandum of Understanding:** A document describing a bilateral or multilateral agreement between parties. It expresses a convergence of will between the parties, indicating an intended common line of action. With respect to information security, it would provide the risk levels of each party (in this case, system), when each system was last authorized, and the DAAs for each system.

**Residual Risk:** The portion of risk that remains after security measures have been applied.

**Risk Assessment:** The process of analyzing threats to and vulnerabilities of an information system to determine the risks (potential for losses), and using an analysis as a basis for identifying appropriate and cost-effective measures.

**Rules of Behavior:** Policies that users agree to abide by before being allowed access to a system.

**Security Test and Evaluation:** An evaluation of all hardware, software, and physical security features that are part of a system. This process involves testing these features to determine what threats and vulnerabilities exist for the system. The findings are documented, and recommendations are made that may be included in the risk assessment.

**Site License Documentation:** A type of software license and a legal agreement that allows users to run the software package simultaneously. In addition, it describes licensing of software to a particular entity which is unrestricted by number, regardless of the physical locations where the software may be used.

**System Development Life Cycle:** A structured approach for systems development from planning and support to disposal of the system. A proven series of steps and tasks utilized to build and maintain quality systems faster, at lower costs, and with less risk.

**System Security Plan:** A set of requirements that are used to delegate how system security will be managed. This plan includes system identification, management controls, operational controls, and technical controls. The system security plan outlines responsibilities for all system users and describes the rules of behavior for those users.

# APPENDIX A – Supporting Information

**Roles and Responsibilities Defined**

The minimum C&A roles include the Designated Approving Authority (DAA), Certification Authority (CA), Information System Owner (Program Manager), Information Systems Security Officer (ISSO), and User Representative. Additional roles may be added to increase the integrity and objectivity of C&A decisions in support of the system business case or mission.

### Designated Approving Authority (DAA)

The DAA is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals. Through security accreditation, the DAA assumes responsibility and is accountable for the risks associated with operating an information system. The DAA should have the authority to oversee the budget and business operations of the information system within the agency and is often called upon to approve system security requirements, system security plans, and memorandums of agreement and/or memorandums of understanding. In addition to authorizing operation of an information system, the DAA can also: (i) issue an interim authorization to operate the information system under specific terms and conditions; or (ii) deny authorization to operate the information system (or if the system is already operational, halt operations) if unacceptable security risks exist. With the increasing complexities of agency missions and organizations, it is possible that a particular information system may involve multiple DAAs. If so, agreements should be established among the DAAs and documented in the system security plan. In most cases, it will be advantageous to agree to a lead DAA to represent the interests of the other DAAs. The DAA has inherent U.S. government authority and, as such, must be a government employee.

### Certifying Authority (CA)

The CA is an individual, group, or organization responsible for conducting a security certification, or comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The CA also provides recommended corrective actions to reduce or eliminate vulnerabilities in the information system. Prior to initiating the security assessment activities that are a part of the certification process, the CA provides an independent assessment of the system security plan to ensure the plan provides a set of security controls for the information system that is adequate to meet all applicable security requirements. To preserve the impartial and unbiased nature of the security certification, the CA should be in a position that is independent from the persons directly responsible for the development of the information system and the day-to-day operation of the system. The CA should also be independent of those individuals responsible for correcting security deficiencies identified during the security certification. The independence of the CA is an important factor in assessing the credibility of the security assessment results and ensuring the authorizing official receives the most objective information possible in order to make an informed, risk-based, accreditation decision. The security category of the information system as defined in FIPS 199 should guide the degree of independence of the CA.

### Information System Owner

The Information System Owner is an agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. The Information System Owner is responsible for the development and maintenance of the system security plan and ensures the system is deployed and operated according to the agreed-upon security requirements. The Information System Owner is also responsible for deciding who has access to the information system (and with what types of privileges or access rights) and ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior). The Information System Owner informs key agency officials of the need to conduct a security certification and accreditation of the information system, ensures that appropriate resources are available for the effort, and provides the necessary system-related documentation to the certification agent. The Information System Owner receives the security assessment results from the certification agent. After taking appropriate steps to reduce or eliminate vulnerabilities, the Information System Owner assembles the security accreditation package and submits the package to the authorizing official or the authorizing official’s designated representative for adjudication.

### Information Owner

The information owneris an agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. The information owner is responsible for establishing the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility even when the information is shared with other organizations. The owner of the information stored within, processed by, or transmitted by an information system may or may not be the same as the information system owner. Also, a single information system may utilize information from multiple information owners. Information owners should provide input to information system owners regarding the security requirements and security controls for the information systems where the information resides.

### Information Systems Security Officer (ISSO)

The ISSO is the individual responsible to the DAA, information system owner, or the senior agency information security officer for ensuring the appropriate operational security posture is maintained for an information system or program. The ISSOalso serves as the principal advisor to the authorizing official, information system owner, or senior agency information security officer on all matters (technical and otherwise) involving the security of the information system. The ISSO typically has the detailed knowledge and expertise required to manage the security aspects of the information system and, in many agencies, is assigned responsibility for the day-to-day security operations of the system. This responsibility may also include, but is not limited to, physical security, personnel security, incident handling, and security training and awareness. The ISSO may be called upon to assist in the development of the system security policy and to ensure compliance with that policy on a routine basis. In close coordination with the information system owner, the ISSO often plays an active role in developing and updating the SSP as well as in managing and controlling changes to the system and assessing the security impact of those changes.

### User Representative

Users are found at all levels of an agency. Users are responsible for the identification of mission/operational requirements and for complying with the security requirements and security controls described in the system security plan. User representatives are individuals that represent the operational interests of the user community and serve as liaisons for that community throughout the system development life cycle of the information system. The user representatives assist in the security certification and accreditation process, when needed, to ensure mission requirements are satisfied while meeting the security requirements and employing the security controls defined in the system security plan.

### Development Lead (DL)

Development Lead serves as the interface between programmers and management and has supervisorial responsibilities in delegating work to the programmers and ensures that the underlying architecture meets the requirements set forth by Management. The DL serves as the mid-point between being a developer and being the solutions architect. The DL at one point was a developer and now instead of coding they are now that part of the puzzle that bridges the vision of the architecture with the reality of the code. In addition, the DL’s mastery of key skills and the ability to look beyond the tasks is able to convert concepts into deliverable solutions. The methodologies and techniques that are employed by the developers are determined and spearheaded by the DL for any given development project.

### System Administrator (SA)

### A System Administrator (SA) is a person who is responsible for managing a multi-user computing environment, such as a local area network (LAN). The responsibilities of the system administrator typically include installing and configuring system hardware and software, establishing and managing user accounts, upgrading software and backup and recovery tasks. The SA maintains the security of the network computers and that all patches and upgrades are performed so that network continues to operate.

### Database Administrator (DBA)

The overall goal of the Database Administrator (DBA) is to ensure the continuous operation of the servers and provide access to users with information when they need it. The DBA is responsible for general maintenance, design and repair on the organization’s database and has a good understanding of the operating system where the database resides. In addition, the DBA ensures that the database is sufficiently protected and all the necessary security measures are in place to safeguard the database to minimize the chance of any data loss. In addition, other DBA activities include replicating data, transferring data, database backup and recovery and controlling privileges and permissions to database users.