UCI FISMA Core
Program Procedures & Processes
Frequently Asked Questions (FAQs)

April 11, 2012
Version 1.1
HAIS Coordination Copy
## REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description of Change</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/14/2011</td>
<td>V 1.0</td>
<td>First Working Edition</td>
<td>Jeff Barnes</td>
</tr>
<tr>
<td>04/11/2012</td>
<td>V 1.1</td>
<td>Second General Reference Edition</td>
<td>Jeff Barnes</td>
</tr>
</tbody>
</table>

# Table of Contents

## Contents

1. Executive Summary ........................................................................................................ 5
   Review and Update Schedule ....................................................................................... 5

2. Background .................................................................................................................. 5
   What is FISMA? .............................................................................................................. 5
   Why is it important now? ............................................................................................. 5
   Does this apply to contracts and grants? ...................................................................... 5
   Why are there different security levels? ....................................................................... 6
   Why is it important to the University of California, Irvine? ....................................... 6
   We already have a contract, so do I have a FISMA requirement? ............................... 6
   What type of language should I look for to determine if I have a FISMA requirement? ........................................................................................................... 7
   Why must my program comply? ................................................................................... 7
   What are the consequences if we don't comply? ......................................................... 7

3. Steps to Achieve FISMA Compliance......................................................................... 7
   What are the steps to achieve FISMA compliance? .................................................... 7
   How long does the process take? ................................................................................ 8
   Who determines if we are compliant? ......................................................................... 9
   How can the University help with the process? ......................................................... 9
   What is a “UCI FISMA Core” and can we leverage it for my individual project? 9
   When using the UCI FISMA Core, which steps must be performed by the
   individual research projects? ...................................................................................... 9
   Where do I get started? ............................................................................................... 10
   What is the UCI FISMA governance structure? ......................................................... 10
   What agreements must be in place? ........................................................................... 10
   What if we decide to pursue an ATO independent of the UCI FISMA Core? ... 10
4. Operational Aspects

- What technology and services does the University provide with the UCI FISMA Core?
- How is the sensitive information protected?
- What operational steps are necessary to leverage the UC Irvine FISMA Core?
- What type of training is required?
- How will it change the way we currently conduct research?
- How will I access the data in the core?
- How can I access UCInet services when I'm connected to the Core?
- Can I print when connected to the Core?
- What type of User Groups will be established?
- How will I identify the Project Lead and User accounts?
- How does the University meet the Continuous Monitoring requirements?
- What happens if there is a security incident?
- Where can I get help?
1. Executive Summary

This *UCI FISMA Core Program Procedures & Processes - Frequently Asked Questions*, or FAQs, define procedures to be used by all users of the University of California, Irvine’s shared research computing environment. This environment, also called the *UCI FISMA Core*, was developed in order to protect sensitive research data created, used, or stored by the University’s research departments. The UCI FISMA Core serves as a secure storage and processing center that can support all University projects requiring a secure environment.

Review and Update Schedule

The is a living document. The HAIS Information Security Officer (ISO) has been designated as the representative of the UCI FISMA Core Information System Owner and Common Control Provider, and is responsible for reviewing and updating following any significant changes to the documented management, operational, and technical security controls.

2. Background

What is FISMA?

The *Federal Information Security Management Act* of 2002 (*FISMA*) is a law requiring protection of the sensitive data either created, stored, or accessed by either the Federal Government or any entity *on behalf of* the Federal Government. The law established a formal Certification and Accreditation (C&A) process that requires a minimum set of security controls and a formal audit prior to obtaining an “Authority to Operate”, or ATO.

Why is it important now?

In April 2010, the Office of Management and Budget issued a Memorandum requiring each Federal Agency to report their FISMA activities to Congress. This memo also reiterated the requirement that Agencies include FISMA requirements in ALL contracts involving sensitive data, as well as grants where sensitive information is created, accessed, or stored *on behalf of* the Federal Government.

Does this apply to contracts and grants?

Compliance with FISMA is mandatory for all contracts and may be mandatory for grants. The decision criteria is based on 1) does the grant require the research organization to return the data back to the Federal project sponsor, and 2) has the grant been awarded using a contracting form.
**Why are there different security levels?**

The FISMA C&A process recognizes that not all sensitive information has the same level of risk and has identified three security categories to identify systems: Low, Moderate, and High. Each level has a mandatory set of security controls, with each level building upon the previous. In addition, FISMA mandates separate evaluations for the **confidentiality**, **integrity**, and **availability** of the sensitive data. The overall system level is the highest of each of the three areas. For example, research data containing individually identifiable health information would pose significant consequences to the University if that data were stolen, lost, or inadvertently disclosed, and thus the confidentiality security category would likely be Moderate. This same historical data may not require 24x7 access so the security category for Availability may be Low. It is often depicted in contracts as:

<table>
<thead>
<tr>
<th>Overall System Security Category</th>
<th>☐ Low</th>
<th>☒ Moderate</th>
<th>☐ High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Impact Levels (High Water Mark)</td>
<td>Confidentiality</td>
<td>Integrity</td>
<td>Availability</td>
</tr>
<tr>
<td></td>
<td>Moderate</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>

Every research project and project sponsor may end up with different security categories, but the basic set of security controls are grouped into Low, Moderate, and High.

**Why is it important to the University of California, Irvine?**

The University of California, Irvine has a number of research contracts from various sources at any one time, representing a sizable financial funding source to the research community. As competition for future research funding increases, those Universities with an existing FISMA compliance program can leverage that advantage into more contracts, and thus increase UC Irvine’s share. Consequently, a failure to meet existing compliance requirements may result in early contract termination and the revocation of contract funds.

**We already have a contract, so do I have a FISMA requirement?**

The 2010 OMB guidance clarifying the Federal Government’s position took several months to disseminate to all Federal Agencies and contracting officers. Previously awarded contracts must also comply, so the University can expect that during the next contract or grant renewal cycle, every contract and certain grants will have FISMA language added. The University has been advised that if the language is NOT present, we should challenge the project sponsor for clarification. A failure to contractually accept the FISMA requirement will not extend deadlines, but only reduce the time we have to comply. Contact the Director of Sponsored Projects or the HAIS ISO if you have any questions on if your project must comply.
What type of language should I look for to determine if I have a FISMA requirement?

The various Federal agencies have different ways to inserting FISMA requirements in contracts and grants. An obvious method is by including a requirement for FISMA compliance in the Statement of Work. This will usually be accompanied with a requirement to submit a System Security Plan (SSP) and a requirement to obtain an “Authority to Operate” from the project sponsor. Other contracts may have Articles titled “Information Security.” There may be a reference to comply with OMB A-130, FIPS 199, or other similar language. Finally, language may be inserted anywhere in the contract stating the project “…will comply with all applicable NIST Standards.” Don’t forget to look at not only the basic contract, but especially in contract modifications or renewals issued in 2010 or later.

Why must my program comply?

Compliance with applicable Federal laws is mandatory. Our Federal sponsors must report to Congress annually on their compliance efforts. If they can’t prove to Congress they are addressing the issue, Congress can withhold research funds. This will in turn result in less research dollars for UC Irvine and hurt our national reputation. Individual programs at UC Irvine that do not comply have already been threatened with a redaction of research funds if they didn’t make progress toward compliance. This issue is viewed as a serious challenge.

What are the consequences if we don’t comply?

If we fail to comply with our sponsor’s requirements, we should anticipate that our research contracts either be terminated by default and/or new contracts cannot be awarded. If a project has a contractual obligation to protect data using the FISMA standards, and a future audit or breach were to occur, serious repercussions can be anticipated leading to loss of future research grant. In certain instances corrective action upon employees may apply as per the required University sanction policy.

3. Steps to Achieve FISMA Compliance

What are the steps to achieve FISMA compliance?

The FISMA compliance path on the surface appears to be complicated. In reality, it can be distilled into three distinct Phases.
• Phase I – Validate the FISMA Requirements, define the certification boundary, and determine the appropriate Security Categories for Confidentiality, Availability, and Integrity¹.

• Phase II - Select and implement appropriate security controls from NIST SP 800-53² based on the Security Category, and then conduct an audit of the controls³, documenting any deficiencies in a Plan of Action and Milestone (POA&M).

• Phase III – Remediate all issues identified in the POA&M and then prepare the certification package for the Designated Accreditation Authority (DAA) (typically your project sponsor) who will issue the Authority to Operate (ATO).

There is also an assumption that the security controls will be continually monitored and adjusted based on periodic risk assessments.

**How long does the process take?**

The length of the FISMA compliance process is highly variable, depending on several factors such as:

• The Security Category (Low, Moderate, High)

• The availability of resources with skills and spare time to manage the process

• The current level of security controls

• The total number of users in a project

• The complexity of the computing environment.

A small project with mature controls and a Low SC can be accomplished in a few months, but a large complex project at the Moderate level may take over a year. Using shared University infrastructures that have already been through the process and have an ATO can shorten the process.

---


² As defined in the NIST Special Publication 800-53 (Revision 3) - *Recommended Security Controls for Federal Information Systems and Organizations*

³ As defined in the NIST Special Publication 800-53A (Revision 1) - *Guide for Assessing the Security Controls in Federal Information Systems*
Who determines if we are compliant?

An independent audit is required for all levels of FISMA compliance. At the University of California, Irvine, that independence may be obtained by having a trained third party either at the University or outsourced, depending upon the complexity. The output of the audit is a Security Test and Evaluation (ST&E) along with the Plan of Action and Milestones (POA&M).

How can the University help with the process?

The University of California, Irvine’s Health Affairs Information Systems (HAIS) has created a secure computing environment to support the University’s research projects. This UCI FISMA Core contains a well-defined certification boundary and shared computing resources that will (eventually) support projects up to the Moderate Security Category level. Because the UCI FISMA Core already has an ATO, much of the paperwork and audit has already been accomplished. Individual projects can get a head start by leveraging the Core.

What is a “UCI FISMA Core” and can we leverage it for my individual project?

The UCI FISMA Core consists of a well-defined security perimeter surrounding a variety of virtual computing resources. All access to the Core is tightly controlled through a dedicated firewall. All data moving between the UCI FISMA Core and the researchers’ computers must be encrypted. Data within the Core is stored on encrypted drives. The Core also comes with the soft security, including those policies, procedures, and administrative support required as part of the FISMA certification process. The following Figure illustrates the Core components.

The UCI FISMA Core is physically inside the UCI HAIS Data Center; however, is separated both physically and logically from the HAIS Data Center outside the Core perimeter. All communications between the project workstations and the UCI FISMA Core are encrypted and just traverse the HAIS network segment and UCInet.

When using the UCI FISMA Core, which steps must be performed by the individual research projects?

While the UCI FISMA Core has completed the C&A process, individual project joining the Core will need to complete an abbreviated set of the same materials. Projects must first establish and document a defined certification boundary. All workstations within the boundary will need to be added to the HAIS domain and a minimum set of security controls implemented. Any servers or databases will need to be ported into the UCI FISMA Core. Project specific paperwork will be needed. The UCI FISMA Core has completed templates so individual projects can start from a known baseline.
Where do I get started?

The first step for any principal investigator to use the UCI FISMA Core is to contact the UC Irvine Director of Sponsored Projects (Nancy Lewis, 949-824-2897, or nrlewis@uci.edu). A quick assessment will be performed to determine 1) the operational requirements and 2) the level of security controls required and in place. At this point, your program will be issued a set of action items to accomplish that may include documentation requirements, additional security controls.

What is the UCI FISMA governance structure?

The UCI FISMA Core received its Authority to Operate from the Vice Chancellor of Research, Dr. James Hemminger. The system is operated by the University’s Health Affairs Information Systems and is under the operational control of the HAIS CIO, Jim Murry. The HAIS Information Security Officer, Jeff Barnes, serves as the UCI FISMA Core ISO. In addition, the project sponsor (usually a Government agency) will serve as the Designated Accreditation Authority (DAA) and will approve the project’s documentation. The HAIS ISO will serve as the liaison between the University and the sponsoring agency.

What will it cost for my project to achieve FISMA compliance?

There are several different aspects for achieving FISMA compliance that involve cost. There are costs for establishing the FISMA Core and incremental costs for adding and maintaining Core participants. There may be costs to bring the workstations used to access the FISMA data up to the required security standards. The cost to the project will depend on factors such as the information system categorization level (Low, Moderate or High), the number of project end users, current security status of the project among others. The cost will need to be determined on a case by case basis.

What agreements must be in place?

In order to use the common UCI FISMA Core, Principal Investigators must comply with the UCI FISMA Core governance structure, adopt and implement all required security controls, and mandate compliance by all authorized users under their authority. The UCI FISMA Core has an approved System Security Plan outlining the minimum security controls. Individual projects must submit a “System Level Controls Appendix (SLCA)” detailing any unique security configurations that are not documented in the UCI FISMA Core. The SLCAs may add additional security controls, but may not reduce the level of security within the Core.

What if we decide to pursue an ATO independent of the UCI FISMA Core?

As Benjamin Franklin said, "We must, indeed, all hang together, or most assuredly we shall all hang separately." Successfully navigating the C&A process takes considerable resources and comes with significant risk to the University, especially if one has not been through the process before. Inexperienced teams historically underestimate the effort and learning curve required to
successfully obtain an ATO. Failures are common and cost additional resources to rearchitect solutions and republish documentation. It is easier to leverage resources and templates that have previously been accepted by our research sponsors.

4. **Operational Aspects**

**What technology and services does the University provide with the UCI FISMA Core?**

Projects with a FISMA compliance requirement must implement not only technical safeguards, but also administrative and physical safeguards. This includes implementing policies and procedures specifically designed to meet the stringent FISMA controls. In addition, in order to remain compliant with FISMA, continuous monitoring and auditing are required to ensure that the safeguards remain effective over time. The University has already implemented the required set of FISMA policies and other safeguards required to remain compliant. The University also has contracts in place for standard security products.

**How is the sensitive information protected?**

The UCI FISMA Core is a self-contained mini-data center within the larger UC Irvine Medical Center’s data center. The outer perimeter meets the security requirements in the Health Insurance Portability and Accountability Act, or HIPAA. The facility is secured with cleared staff. Emergency generators and uninterruptable power provide a safe environment. Data is automatically backed up on encrypted tapes and stored off-site.

**What operational steps are necessary to leverage the UC Irvine FISMA Core?**

Adding a research project to the UCI FISMA Core first requires all users to be on the HAIS Active Directory Domain. Operational control of the workstations will then be managed by the FISMA Core team. All workstations that will access the Core must be encrypted unless there are specific justifiable reasons, but only then after appropriate compensating controls will be applied that have been pre-approved by both the HAIS team and the project sponsor (e.g., NIH, DoD).

**What type of training is required?**

All users must successfully complete the UCI FISMA Training, which includes reading and comprehending the information in this document. This document is designed to supplement, not replace all other mandatory user training directed from UCOP, UC-Irvine, and HAIS.

Users are reminded that external project sponsors will often have other mandatory training requirements that are unique to the sponsor.
How will it change the way we currently conduct research?

Regardless if the project uses the FISMA Core or not, all project workstations that have access to sensitive data must be encrypted with a pre-boot encryption package, have a minimum set of security controls enabled, and have passwords reset every 60 days. There are generally no additional operational changes beyond what is already required by FISMA.

How will I access the data in the core?

All access to the UCI FISMA Core will be through a secure SSL/VPN connection. Projects that only require personal and shared storage will map to similar H: (Home) and S: (Shared) directories. The difference is that those directories will be physically located in the secured facility and encrypted. For projects that require a computing environment, virtual desktops will be created containing the required project applications. Access to the virtual desktops will be through secured remote connections. Fiber connectivity between the main UC Irvine campus and the Medical center has been established to ensure virtually indistinguishable performance changes.

How can I access UCInet services when I’m connected to the Core?

The connection to the UCI FISMA Core (e.g., H: and S: drives) is exclusive. The connection, when active, disables all other network functions to prevent an accidental release of sensitive data to non-trusted devices. While connected to the Core, you will not be able to print, send, or receive e-mail, or connected to other shared drives or services.

There is a technical restriction stopping printing when a workstation is connected to the UCI FISMA Core. In this instance, access to the rest of the campus network, including the print servers, will be temporarily suspended while the workstation is connected to the UCI FISMA Core. Printers & and print servers will be automatically connected again when the UCI FISMA Core connection (e.g., unmounting the H: and S: Drives) is terminated.

Can I print when connected to the Core?

Printing of data and reports subject to FISMA is not permitted by policy, unless the printer is included within the individual project’s certification boundary. You Principal Investigator made the determination at the beginning of the project on if the printers were needed. The reason that printing is not normally allowed is that FISMA requires an auditable physical perimeter, and UCI printers are not normally located in secure areas.

Printing of non-FISMA-controlled documents is allowed by policy, but cannot be accomplished when connected to the UCI FISMA Core. Printing to local devices (e.g., USB desktop printers) will not be impacted at any time; however, users must comply with the printing restrictions as documented for their respective research project.
What type of User Groups will be established?

Each research project’s Principal Investigator will be required to identify “project leads” and “users.” The project leads are those designated individuals within a research project who are ‘authorized’ to submit change request to add, modify, and remove users from the project. Project leads will also periodically review audit logs to ensure all access to the data was authorized. Users are all other individuals working on the project that have been granted access to the project resources.

How will I identify the Project Lead and User accounts?

All Project Lead accounts will be issued local administrator credentials on their workstations. Project Leads will be issued dual credentials as both Project Lead and User. The name for both accounts will follow the naming convention EXCEPT the administrator accounts will contain a “!” or ‘bang’ before the name. For example, John Smith’s user account will be jsmith@uci.edu, while John Smith’s administrator account will be “!jsmith@uci.edu” which includes the bang. Project Leads should only use the Project Lead (administrator) account with performing auditing. Normal day-to-day operations can be performed using the User accounts. Project Lead accounts will have a higher level of auditing and external monitoring.

How does the University meet the Continuous Monitoring requirements?

All FISMA projects have a requirement for continuous monitoring. The UCI FISMA Core has deployed several tools to monitor for intrusions and unauthorized activities. Help desk staff are available 24x7 for high priority emergencies.

What happens if there is a security incident?

FISMA requires a robust security incident response process. The continuous monitoring tools will alert the help desk staff if an event reaches pre-defined thresholds. All project staff will be expected to immediately report security incidents to the HAIS help desk. If an event is traced to one of the project’s computers, the principal investigator and the user will be expected to fully cooperate with the investigation. The system may be temporarily removed from the network to project the integrity of the environment.

Where can I get help?

The first place to obtain general information is the HAIS Information Security Officer, Jeff Barnes, at 714-456-7349 or jlbarnes@uci.edu.