

**Federal Information Systems Management Assessment Tool for Intelligent Compliance** (FISMAtic)

**Proof of Concept Documentation**

Final

Version: 2.0

Date: 6/8/2020

| **Version** | **Publication Date** | **Revision Description** | **Section** | **Author** |
| --- | --- | --- | --- | --- |
| 0.1 | 2/19/2020 | Initial | All sections of document | Stacie Whitesides |
| 0.5 | 4/02/2020 | Updated entire document based on initial review meeting with CAT Deputy Program Manager | All sections of document | Stacie Whitesides |
| 1.0 | 4/13/2020 | Updated entire document based on review with CAT team | All sections of document | Stacie Whitesides |
| 1.5 | 5/12/2020 | Revisions made based on updates to FISMATIC tool | Reference Page  Section(s) 4, 5.2, 6 | Stacie Whitesides |
| 2.0 | 6/8/2020 | Revisions made based on internal PoC Team Review | All sections | Stacie Whitesides |

**Document History**

**Table of Contents**

[**1 Executive Summary** 4](#_Toc42505654)

[**2 Introduction** 4](#_Toc42505655)

[**3. POC Overview** 5](#_Toc42505656)

[**3.1 Current POC Capabilities** 5](#_Toc42505657)

[**4 Authority to Operate (ATO) Overview and PoC Solution** 5](#_Toc42505658)

[**4.1 Authority to Operate Interviews and Lessons Learned** 5](#_Toc42505659)

[**5.1 FISMAtic Functionality** 7](#_Toc42505660)

[**5.2 FISMAtic Encryption** 9](#_Toc42505661)

[**6 Current Status and Next Steps** 10](#_Toc42505662)

[**Acronyms and Terms** 11](#_Toc42505663)

[**Appendix B** 12](#_Toc42505664)

[**Information Security, Guidance, and Governance** 12](#_Toc42505665)

[**Appendix C FISMATIC Public GitHub Reference Page** 13](#_Toc42505666)

# **1 Executive Summary**

The purpose of this document is to introduce the Federal Information Systems Management Assessment Tool for Intelligent Compliance (FISMATIC) proof of concept (PoC) developed by the Census Bureau Center for Applied Technology (CAT). This machine learning PoC sets out to assist and streamline the bureau’s Authority to Operate (ATO) process. The CAT seeks to develop a PoC that demonstrates a tool that will improve the process of certifying the security and compliance of bureau information systems by reducing costs, speeding time to completion, and improving consistency with machine learning, and natural language processing.

# **2 Introduction**

The vision behind the PoC team development of the tool is to l assist in the completion of the ATO packages and streamline the assessment process. FISMATIC seeks to increase the quality of the responses and supporting material against each applicable control in the National Institute of Standards and Technology (NIST) Special Publication 800-53, as well as improve the initial control selection process, greatly reducing the Office of Information Security (OIS) assessor and System Owners (SO) workload. Once in place, this tool will streamline ATO processes while also reducing system deployment timeframes and costs.

The NIST SP 800-53 specifies seventeen control families and almost 1500 controls in its entirety. At the Census Bureau, a recent ATO spreadsheet developed by OIS details roughly 58,000 rows of controls and response documentation. As the bureau modernizes Information Technology systems, new systems will each require an ATO.

**NIST Special Publication 800-53 Control Families**

|  |
| --- |
| **Control Families** |
| Access Controls |
| Audit and Accountability |
| Awareness and Training |
| Security Assessment and Authorization |
| Configuration Management |
| Contingency Planning |
| Identification and Authentication |
| Incident Response |
| Maintenance |
| Media Protection |
| Personnel Security |
| Physical and Environment Protection |
| Planning |
| Risk Assessment |
| System and Communications Protection |
| System and Information Integrity |
| System and Services Acquisition |

# **3. POC Overview**

FISMATIC is currently being developed as a proof of concept in an iterative Agile process. The PoC team is ensuring that all main objectives are being captured and using feedback received from various Information System Security Officer (ISSO) ISSO’s to improve the tool. The CAT PoC team developed a Memorandum of Understanding (MOU) between the CAT PoC team and OIS to provide the CAT PoC team with access to sensitive ATO data and information. To continue the development of the PoC for FISMATIC there will need to be solid stakeholder buy-in.

Pilot testing has begun with bureau system owners and assessor teams that have ATO process experience. The PoC team is currently working to develop a test plan that will formally outline the process of FISMATIC pilot tests.

## **3.1 Current POC Capabilities**

While the full development of FISMAtic is important to the bureau, based on an assessment of tools available at the Census Bureau and the resources provided for the PoC development there are a few key objectives that will need to be vetted and implemented first to advance the development of the tool.

The two main objectives that the FISMAtic tool will address are:

* Development of User Responses

## **4 Authority to Operate (ATO) Overview and PoC Solution**

An ATO is the official decision by the Bureau CIO and senior management to authorize operation of an information system and to formally accept any risk associated with the implementation of the agreed upon security controls as required by NIST Special Publication (SP) 800-53. See the chart below for a complete list of the NIST SP 800-53 Control Families. See Appendix B for more information about Information Security, Guidance and Governance.

## **4.1 Authority to Operate Interviews and Lessons Learned**

At the end of 2018, there were a series interviews conducted to understand the current ATO process across the Federal government and contractors. There were 22 people interviewed across a vast group of federal agencies as well as the private sector. The different organizations that were included in the interview process were:

* [Centers for Medicare and Medicaid (CMS)](https://www.cms.gov/)
* [General Services Administration (GSA)](https://gsa.gov/)
* [National Geospatial-Intelligence Agency (NGA)](https://www.nga.mil/)
* [United States Air Force](https://www.airforce.com/)
* [CivicActions](https://civicactions.com/)
* [Epigen Technology](http://epigentechnology.com/)
* [GovReady](https://govready.com/)
* [Onyx Point](https://www.onyxpoint.com/)
* [Telos](https://www.telos.com/)

**Note**: Additional interview background information can be found on the FISMATIC GitHub site.

The basic process for an ATO is summarized as below.

**Step 1**: The system owner creates an ATO documentation package that indicates how the system meets NIST SP 800-53 security and privacy controls (SP 800-53 identifies the required controls depending on the risk level [low, moderate, high] of the system).

1. This documentation contains written responses for each control
2. This documentation may contain supporting documentation such as screenshots or manuals

**Step 2**: An information security assessor examines each control and its supporting documentation. A pass / fail is associated with each response at the control level.

1. At this point a back-and-fourth conversation is held over any failed controls

**Step 3**: An overall score is created and a recommendation is made to the Chief Information Officer (CIO)

**Step 4**: The CIO either accepts the risk or rejects it.

Note: These steps within the process may vary based on the business that is creating the ATO at the time.

There were six major findings that came out of the interviews, those findings are listed in the table below.

|  |  |
| --- | --- |
| **Category** | **Response Details** |
| Program teams are not well-equipped to complete ATOs | Lack of working knowledge of NIST terminology  Inexperience in the area of compliance.  The length, and access to ATO templates and examples. |
| Prioritization of security/compliance work is critical | Compliance is a byproduct of good information security and having experienced security subject matter experts on program teams is essential to the success of developing ATOs. |
| Low (perceived) value of compliance work by program teams | Security and privacy is the main concern of the security assessors. Their low value of compliance work may be due to the lack compliance knowledge. Resources may not be the same, the creators of the ATO’s and the developers/users may differ. |
| Collaboration between program teams and assessors. | Both program teams and assessors being available, and willing to share experiences in writing ATO’s. |
| Power and confusion in inheritances | Understanding and acknowledging when or if controls should be inherited, this could cut down on the amount of time it takes to complete an ATO.  OpenControl is a tool that is often used |
| Knowledge of compliance tools | There are various tools available to assist with documenting compliance workflows; however, most times these tools are not used (or used in full capacity) and instead replaced by Microsoft Word. |

## **5.1 FISMAtic Functionality**

FISMAtic has been developed as a Python program with a Tkinter user interface. The sensitive ATO data is downloaded from Risk Management Program System as a CSV, and then is cleaned and modified before being loaded into FISMAtic. The tool then organizes the control steps and provides step by step recommendations based on successful ATO’s and user input. The FISMAtic process:

**1**: Upload data file

**2**: Shows User 2 sample responses based on prior answers

**3**: Allows the user to edit responses or input their own response

**4**: Enables user to save response and continue with next step

The two figures below illustrate the current user interface.



**Figure 1: Navigation Page**

On the left side a button is created for each control family present in the CSV file.

Color Key:

Grey: Not Started

Pink: Partially Complete

Blue: Completed

Red: Currently Selected

**Upload File:**

This opens a user’s File Explorer to select a new CSV file to run through FISMATIC - navigation page with refresh once uploaded.

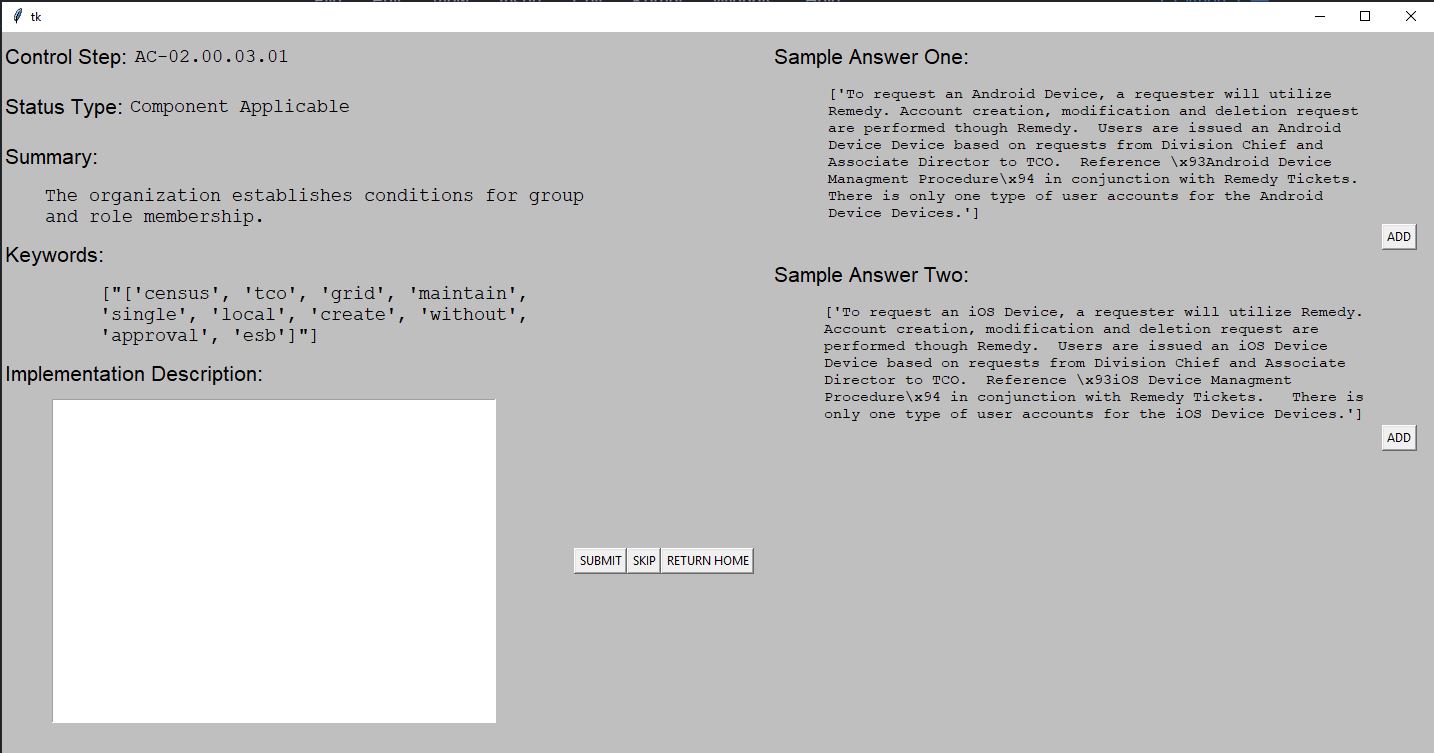
**Start!:**

Begins running FISMATIC through the controls of the currently selected control family.

**DONE:**

This exports a new version of your CSV file with your responses added.

Exports as: "fismatic\_MM\_DD\_YYYY\_HH\_MM.csv"



**Figure 2: Control Response Page**

This shows your current control step and its status type. It shows a summary of control itself and has a space of a user’s response.

The buttons work as followed:

**SUBMIT:** saves your response and moves on to next control step.

**SKIP:** Does not record a response, moves on to next control step.

**RETURN HOME:** Saves responses you've made so far and saves your place in the set of controls.Returns you to the navigation page.

On the right side you see Two Sample Responses that are extracted from successful ATO's that other users have created in the past.

The ADD buttons copy and paste the response into the text field, where they can be edited before submission.

## **5.2 FISMAtic Encryption**

FISMATIC has been updated to include symmetric encryption, which uses one key for encryption and decryption. The capability was added to ensure only FISMAtic can use the sensitive Data, the encrypted Data files cannot be read by the users.

FISMATIC Encryption Steps:

1. User will receive file attachment labeled “key.key”
2. User will be prompted to upload file when FISMATIC is running
   1. The key is prompted to decrypt the data and to be open by FISMATIC

# **6 Current Status and Next Steps**

Next Steps for FISMAtic:

1. Field Guide Information Pop-up
2. Refresh Sample Answers Button
3. View Previous Response
4. Reuse a Previous Response
5. Stakeholder buy-in
6. MOU is being updated to enableread-onlyaccess to the Risk Management Program System (RMPS)
7. Access to RMPS
8. Review the RMPS control selection process and customized exports for past ATO packages
9. Obtain more samples of ATO documentation packages to use for training and enhancing the machine-learning model
10. Finish POC development and pilot testing
11. Work with ITD to plan the deployment and adoption of FISMAtic in production environment.

**Appendix A**

# **Acronyms and Terms**

|  |  |
| --- | --- |
| **Acronym** | **Term** |
| ATO | Authority to Operate |
| CAT | Center of Applied Technology |
| CIO | Chief Information Officer |
| FISMATIC | Federal Information Systems Management Assessment Tool for Intelligent Compliance |
| ISO | Information Security Office |
| ISSO | Information System Security Officer |
| ITD | Information Technology Department |
| IOT | Internet of Things |
| MOU | Memorandum of Understanding |
| NIST | National Institute of Standards and Technology |
| POC | Proof of Concept |
| RMPS | Risk Management Program System |
| SP | Special Publication |

# 

# **Appendix B**

# **Information Security, Guidance, and Governance**

**Information Security**

Overall security is a major part of how we get, store and disseminate information. Information Security specifically pertains to the processes designed for data security and is also an important part of Cybersecurity. Cybersecurity is the process of protecting systems, networks and programs from cyber digital attacks. Such attacks aim to compromise and intercept data that is stored within financial institutions, government agencies, personal devices and other objects belonging to the internet of things (IOT). In the next sections we will delve deeper into why information security is important to the Census Bureau.

**Information Security Guidance and Governance**

The National Institute of Standards and Technology informally known as NIST was developed in 1901 by Congress to eliminate major challenges to the United States industrial competitiveness. Now NIST is an expanding part of the United States Department of Commerce, and today supports a wide array of technologies, from the largest most complex creations to the nanoscale devices and networks. NIST is responsible for developing standards and guidelines, including minimum requirements and for providing adequate information security for all agency operations and assets, but not all standards and guidelines may not applicable to national security systems. These guidelines have been prepared for use by federal agencies and may also be used by non-governmental organizations on a voluntary basis.

# **Appendix C FISMATIC Public GitHub Reference Page**

FISMATIC research and background information can be found on the FISMATIC Public GitHub page at [uscensusbureau/fismatic](../../../../:w:/r/sites/FISMATIC413/_layouts/15/Doc.aspx?sourcedoc=%7BE1A0DD26-B4E3-410A-9052-10B9DB61DA81%7D&file=FISMAtic%20PoC.docx&action=default&mobileredirect=true)

Top of Form