CEM IR&D 2007

Secure Citizen Interaction Framework

FINAL

Version 1.0

February 6, 2008

Principal Investigator
Clarke Thomason

Co-Author
David Carroll

MITRE
Center for Enterprise Modernization
McLean, Virginia

FEDERALLY FUNDED RESEARCH AND DEVELOPMENT CENTER
THE MITRE CORPORATION
Secure Citizen Interaction

Executive Summary

This document outlines a generalized framework to investigate a potential approach for a United States Government Agency's use of a secure channel for interacting with Citizens.

Background

The interest in a Secure Citizen Channel applies to many agencies of government, including the Census Bureau, Internal Revenue Service (IRS), General Services Administration (GSA), Social Security Administration (SSA), Department of Homeland Security (DHS), Centers for Medicare & Medicaid Services (CMS), and others. Many alternative design solutions have been tried by different agencies with varying degrees of effectiveness. The MITRE Corporation (MITRE) has participated in several related cross-government working groups that provide specific technical information and real world benefits in this area.

Hypothesis

The hypothesis for this research is that it is possible to integrate a set of existing guidelines and technologies to architect and specify an operationally secure, risk-balanced, and effective Citizen's Interaction Channel. This set of technologies could include a method to assure that a personal system used by Citizens will not compromise the channel's security.

This document formulates a generalized approach to the process an agency could take to establish a secure channel over the internet that will interact with Citizens. Sample requirements and representative business processes are defined, assumptions documented, and a baseline technical architecture presented as a baseline "Model" design set for use as a base of analysis. This Model is then evaluated along with potential solutions.

A representative set of data that would be collected from Citizens, maintained, shared, or disseminated is defined, as well as how this information set might be used. The sensitivity level associated with the representative information was also ascertained. A privacy impact assessment of collecting and maintaining this information is then presented.

Research

MITRE's research looks into potential solutions and technologies to maintain the channel's usability balance. Based on the sensitivity of the collected data and the operational scenario, this analysis presents approaches to e-authentication of Citizens that is appropriate for the required level of assurance. The Citizen's options for use of the channel are considered.

Included in the final deliverables of this Internal Research and Development (IR&D) effort are a strawman design and a prototype Model system description that demonstrates the integration of technologies in support of the developed framework. Several key risk issues that were identified in this research have been investigated for mitigation.

The final segment of this research is an investigation and demonstration of two key technology elements of a potential solution—Authentication and Citizen Computer Platform Validation. This research provides a structured approach to MITRE's findings by component area, a focus on the significant areas of challenge encountered, and MITRE's identified alternatives and recommendations.

There is also a set of existing federal component standards, guidelines, and orders available to define and specify the minimal requirements for fielding an effective and compliant Secure Citizen Channel Program. The current challenges of multiple, sometimes conflicting, agency-specific security guidance can be effectively overcome by a systematic application of available NIST, FISMA, FIPS, OMB, or other federal standards and guidance.

In summary, while there are still significant challenges not mitigated directly in this research, it is clear that there are emerging technologies that could significantly reduce the risk of implementing these Secure Citizen Channels. Overall, many of the major weaknesses and security risks can be contained with some creative and tailored COTS solutions for the specific government security requirements as outlined in the "Moderate" Model defined in this research. However, some solutions require a forward-looking anticipatory approach to security design versus the traditional security problem and reactive mode of design and operations. Helping the Citizen to better secure an inherently unsecured Citizen PC is one example.

The operation and support aspect of the Secure Citizen Channel is out of this IR&D's scope.

Table of Contents

List of Figures

List of Tables

1. Abstract and Value Proposition

1.1 Background

Many government agencies require a secure, authenticated, and reliable channel to and from the Citizen for Information exchange.

Complete, clear, and concise government procedures and specifications are not currently available in one document. One document would provide a totally integrated single set of lifecycle guidance for all phases (i.e., from scope and conceptual approval through implementation, to operational risk assessment, and finally to implementation and operations) for this type of communications channel. Although current discrete standards, requirements, and guidance memoranda are available, MITRE preferred to document an example process in one document. As one step in this research, MITRE reviewed alternative solutions that have been tried by different agencies with different degrees of effectiveness and success using these standards. In addition, MITRE is participating in several related cross-government working groups that share information and benefit from this work.

In this cross-government work, the need for this channel has been shown to potentially apply to many government agencies, including the Census Bureau, eVoting, the Internal Revenue Service (IRS), the Social Security Administration (SSA), and many others.

The government needs an example of a repeatable, reasonable process and methodology to map this process clearly. MITRE's goal was to help facilitate this process by creating a sample run of the various processes, to identify major risks, and to determine if potential mitigations existed in current technology for some of the key risk areas. With a structured run through this existing methodology, MITRE hopes to do the following:

- Provide an example that will help facilitate the design and implementation process for government agencies
- Balance this demonstration of the Modeled process with realistic risks and challenges found
- Provide possible solutions associated with this type of Citizens Interface and Data Collection Channel

1.2 Research Objective

The idea for this research is to integrate the set of existing federal regulations and standards with available best practices in methods, processes, and technologies, as well as to walk through this structured example to create, document, and demonstrate an operationally secure and effective channel that meets existing standards. This work will assemble a set of data, references, and tools to explore the concept and reasonable process to evaluate and document the balance between security, operational risk, scope, and cost. MITRE's findings will identify critical focus areas for a "typical" Secure Citizen Channel.

1.3 Technical Idea/Research Hypothesis

It is possible to integrate and walk through a set of existing regulations, standards, processes, and technologies in a well-defined and traceable process to document and demonstrate an operationally secure, risk balanced, and effective Citizens communications channel example.

1.4 Impact

This research effort has helped the Center for Enterprise Modernization (CEM) extend MITRE's expertise in Secure Citizen Channel applications and technology. It has also established new relationships with other authentication, security, and communications channel technologists in the government, private sector, and MITRE, which can be leveraged to solve new classes of problems for Citizen customers.

It is MITRE's intent that the results of this research will have direct applicability to similar efforts at the Census Bureau, IRS, General Services Administration (GSA), SSA, and many other Civil agencies. Many agencies are in need of a sample process roadmap for existing technologies that can be used to create an operationally secure and effective channel. Conducting this research has helped MITRE demonstrate and fulfill its commitment to identify and support critical federal government needs, to support those organizations when possible, and to better serve the citizen.

1.5 Value Proposition

MITRE's existing Citizens Contact Channel expectations research and interactions with government clients show that there is significant demand for a blend of secure, trusted contact channels to and from the Citizen. The internet is one of the leading expectations for a trusted channel to the government from the Citizen. A consolidation and sample walk through of existing guidance, specifications, and processes will help to outline that a reasonable set of methods and processes for justification, design, approval, implementation, and certification for operations exists. This example could in turn help to speed the implantation of trusted and efficient citizens Contact Channels. These channels could provide an increased speed of input from the Citizen, at reduced costs, and positively impact the Citizen's expectations for accuracy and efficiency in government interactions.

2. Summary of Research Approach

The approach to this research is based on five (5) key phases or steps. Figure 1 outlines a process roadmap for these phases. These key phases would be useful and applicable to any Citizens Interactions Project definition.

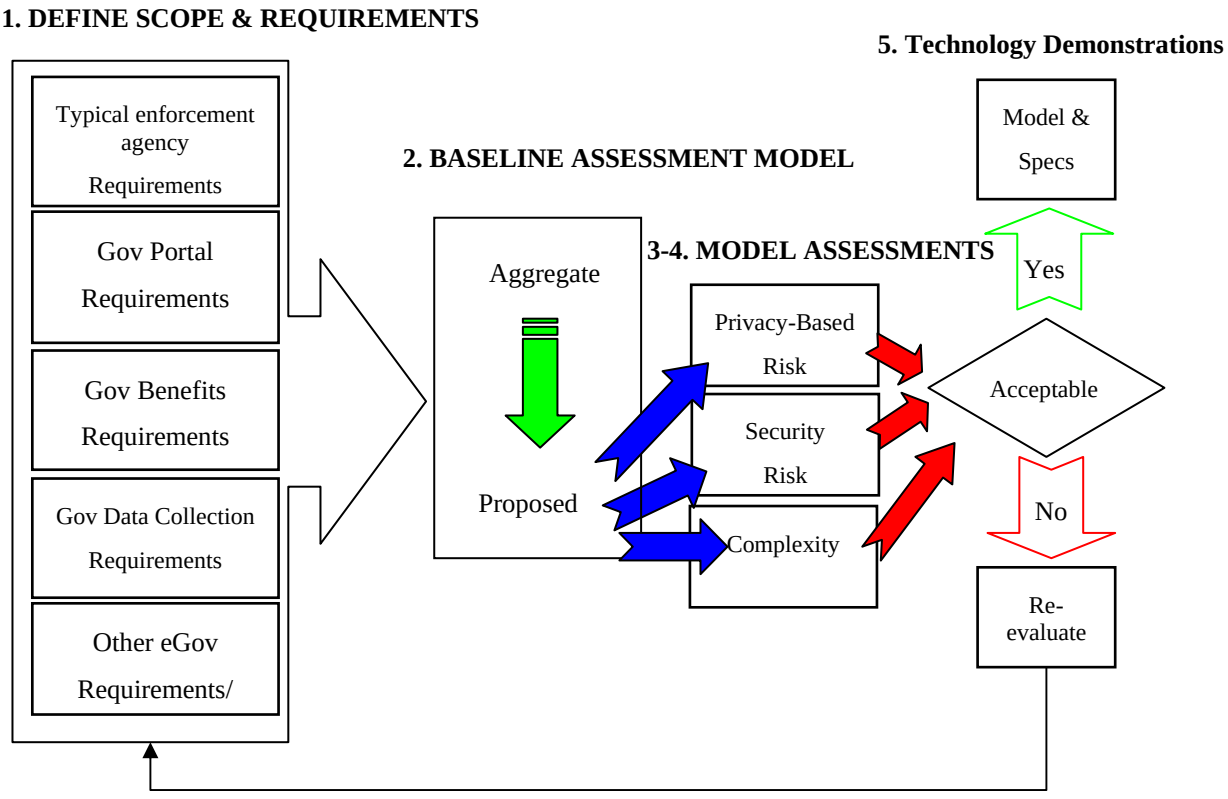

Figure 1. Research Process Roadmap

2.1 Phase 1—Define Scope and Requirements

Phase 1, Define Scope and Requirements, is centered on defining an appropriate and reasonable scope for the research project. This phase also examines similar federal programs and systems to review and collect similar Civil Citizens Interactions requirements. By reviewing these requirements and then selecting a reasonable and representative scope of investigation that fits within the limited funding and resources of this research program, MITRE can then define a baseline scope for the business, operations, data, performance, and other core requirements. This core scope definition will guide and bound the requirements to form the baseline set of requirements used in MITRE's generic baseline Model for this research.

2.2 Phase 2—Define Baseline Design and Assessment Model

Phase 2, Define Baseline Design and Assessment Model, is used to define Model details for this effort within the aforementioned research scope. For this research, MITRE's baseline is defined

as a "Model" because it is meant to be a generic set of assembled requirements, specifications, and operating parameters, from similar Civil agency needs, to allow the process outlined in this research to be applied to it. In a specific systems implementation, this "Model" would be replaced by the requirements for the specific Citizens Interaction Channel being deployed.

2.3 Phase 3—Privacy and Sensitivity Risk Assessments

Phase 3 is the Privacy and Sensitivity Risk assessment of the channel and its data—a key step in the data risk/security balance and design. The level of security required must be assessed early in the process.

2.4 Phase 4—Security Risk Assessments

Phase 4 is a security risk assessment of the model design. This step will assess the classic technology risk factors and recommend a balanced secure technology approach.

2.5 Phase 5—Technology Demonstrations

Phase 5, Technology Demonstrations, is based on a strawman technology architecture and consists of a demonstration of key technology concepts. This technology demonstration will be a simple investigation of these select key concepts and will provide sample candidate technologies to apply to the significant top risk areas that emerged in the analysis of the baseline Model. MITRE's goal is to demonstrate at least two or three major new or emerging technology innovations that contribute to mitigating the most significant risk areas for this type of Secure Citizens Channel, which emerged from the design's privacy, threat, and security analysis.

2.6 Summary Assessment

The final phase is a summary assessment of findings and value of potential practices and technologies for future programs. All programs must be sufficiently complex to be effective; yet efficient enough to survive today's tight federal budgets. This section will outline final thoughts and observations from MITRE's research and technology investigations.

3. Overview of Similar Research

Previous work in this area of research generally fell into the following three areas.

1. Citizens Expectations for Contacting the Government
2. Component Communications and Security-Related Research
3. Other Similar Secure Channel Programs

3.1 Citizens Expectations for Contacting the Government

The first area of related research defines the business needs and performance expectations from Citizens for this type of interactive secure communications channel. For security and client-confidentiality reasons, these specific programs must be summarized, yet not specifically referenced in detail in this document.

MITRE completed related work with GSA during the last year on understanding current Citizens Contact Channels and produced strategic plans, cost Models, best practices, quality and performance benchmarks/metrics, and detailed focus group research on Citizens expectations for these Government Contact Channels. This successful work has resulted in MITRE's research being published by GSA as a benchmark on its website. The Citizens Contact Channels' expectations information has also been cited by IRS in its Taxpayers Assistance Blueprint work. Both of these previous work efforts form a baseline of understanding "user" needs and expectations for a Secure Citizen Contact Channel.

In summary, this research indicated that there are an ever-growing expectations for a secure, efficient, and convenient Citizen Internet Interaction Channel. This research outlines that demographics spread across age, income, and education are looking for a balanced and interdependent array of options for contacting the government for information and services. A secure internet channel is one major Citizen expectation.

3.2 Component Communications and Security-Related Research

The next area of related work centers around several specific technology component "focus" areas.

Many existing "technology only" focused efforts have been attempted with various levels of successes and failures in recent years. MITRE has gained great experience across Federally Funded Research and Development Centers (FFRDC) in programs and MITRE labs with many of the researches' component technologies. For example, in the areas of authentication, data security, risk assessment, vulnerability analysis, and pilot implementations, MITRE has significant and proven internal expertise available from across MITRE.

The risk of focusing on only one specialty area or approach is that these previous efforts tended to focus on individual component technologies and not the overall process and integrated methodologies required to deliver balanced complex integrated solutions to meet specific citizen and government business and budget needs successfully and effectively. A risk, security, complexity, and usability balance must be defined.

3.3 Other Similar Secure Channel Programs

The third area of related work MITRE reviewed for this research was review various other channel programs and their successes and failures. Many of the most successful efforts have been highly specialized, have had many restrictions, and were at a relatively-high cost per Citizen user. The IRS and its eFiling is an example of a success story with steady growth and acceptance. MITRE has been involved with reviews and assessments of the Registered User Portal and the related development and upgrades of the Modernized IRS eFile. MITRE is also working currently with the National Institute of Standards and Technology (NIST) on several security standards evaluation and support projects.

Some programs that have failed in this segment were technically successful in prototype phases, but then failed in final implementation due to a lack of documentation, solid business and risk cases, usability, cost control, and political buy-in.

Many of the technology problems were often overcome; however, the programs required more then solid individual technology components. A balance of realistic security requirements, usability, threats, and costs is required. This balanced overall implementation approach must contain appropriate security designs and requirements for business processes and data sensitivity, matched with cost-effective and balanced levels of mitigation. These must then be traceable to a documented federal process and set of specific standards so the programs can be accredited for operations and complete to implementation/Citizen Service. A critical balance of key NIST, Office of Management and Budget (OMB), and other government agency (OGA) requirements is required for the formulation of a workable and dependable risk and cost balance. Many of the early prototypes were not successful because they did not have this balance. Some failed because they had inadequate security designs, some for a lack of traceability to standards, some did not cover major threats, some had cost overruns, and finally some for being too burdensome for operations and users.

4. Identified Core Federal Standards and Guidance

MITRE reviewed the applicable standards and guidance from the federal government and other sources. Relevant information used as major references is outlined by area in this section. MITRE based its work on the core NIST 800-53 information as a foundation and then supplemented with information and guidance from NIST, OMB, and other federal and private sources, as required.

4.1 NIST Standards and Guidelines Compliance

A general introduction and overview of the compliance process, as required by the Federal Information Security Management Act (FISMA, 2002, P.L. 107-347), can be found in the *Guide for Assessing the Security Controls in Federal Information Systems* (NIST 800-53, June 2007) review draft:

- "NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act (FISMA) of 2002 and in managing cost-effective programs to protect their information and information systems."
- "Federal Information Processing Standards (FIPS) are developed by NIST in accordance with FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use."
- "Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget (OMB) policies (including OMB FISMA Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that for other than national security programs and systems, agencies must follow NIST guidance."
- "Other security-related publications, including interagency and internal reports (NISTIR) and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when so specified by OMB."

4.2 NIST Standards and Guidelines Schedule for Compliance

- "For legacy information systems, agencies are expected to be in compliance with NIST security standards and guidelines within one year of the publication date unless otherwise directed by OMB or NIST."
- "For information systems under development, agencies are expected to be in compliance with NIST security standards and guidelines immediately upon deployment of the system."

4.3 Implementing Security Standards and Guidance

An overview of the requirements review process, as required by the Federal Information Security Management Act (FISMA, 2002, P.L. 107-347), can be found in the *Guide for Assessing the Security Controls in Federal Information Systems* (NIST 800-53A, June 2007) review draft:

- "FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, is a mandatory, non-waiverable standard developed in response to the Federal Information Security Management Act of 2002. To comply with the federal standard, agencies must first determine the security category of their information system in accordance with the provisions of FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, and then apply the appropriate set of baseline security controls in NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems. Agencies have flexibility in applying the baseline security controls in accordance with the tailoring guidance provided in Special Publication 800-53. This allows agencies to adjust the security controls to more closely fit their mission requirements and operational environments."
- "The combination of FIPS 200 and NIST Special Publication 800-53 requires a foundational level of security for all federal information and information systems (other than national security information and information systems). The agency's risk assessment validates the security control set by determining if any additional controls are needed to protect agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, or the nation. The resulting set of security controls establishes a level of "security due diligence" for the federal agency and its contractors."
- "In addition to the security requirements established by FISMA, there may also be specific security requirements in different business areas within agencies that are governed by other laws, Executive Orders, directives, policies, regulations, or associated governing documents, (e.g., the Health Insurance Portability and Accountability Act of 1996, the Federal Financial Management Improvement Act of 1996, or OMB Circular A-127 on Financial Management Systems). These requirements may not be equivalent to the security requirements and implementing security controls required by FISMA or may enhance or further refine the security requirements and security controls. It is important that agency officials (including authorizing officials, chief information officers, senior agency information security officers, information system owners, information system security officers, and acquisition authorities) take steps to help ensure that: (i) all appropriate security requirements are addressed in agency acquisitions of information systems and information system services; and (ii) all required security controls are implemented in agency information systems when determining the tailored and supplemented control baselines described in NIST Special Publication 800-53."
- "See http://csrc.nist.gov/sec-cert/ca-compliance.html for additional information on compliance."

4.4 Additional Key References and Requirements

General Technology Security

- Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347:
  - OMB Circular A-130 *Management of Federal Information Resources*, Rev. 4.
- NIST 800 Series Security Guidance for Information Technology (IT) Systems:
  - NIST 800-53, *Minimum Security Controls for Federal Information Systems.*

– NIST 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, Draft, June, 2007.

Security Level Determination

- NIST 800-12, *An Introduction to Computer Security: The NIST Handbook.*
- NIST 800-60, *Guide for Mapping Types of information and Information Security to Security Categories*, June 2004.

Security Categories and Impact Analysis

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

eAuthentication

- NIST 800-63, NIST Special Publication (SP) Version 1.0.2 *Electronic Authentication Guideline Recommendations of the National Institute of Standards and Technology*, April 2006.
- OMB M-04-04, *E-Authentication Guidance for Federal Agencies*, December 16, 2003.
- OMB 06-16, *Protection of Sensitive Agency Information*, June 23, 2006.

Communications Security

- FIPS 140-2, *Security Requirements for Cryptographic Modules*, December 3, 2002.

Risk Assessment and Mitigation

- NIST 800-30, *Risk Management Guide for Information Technology Systems*, July, 2002.

Security Controls

- FIPS 200, *Minimum Security Controls for Federal Information Systems*, Fall 2005.
- NIST 800-53, *Recommended Security Controls for Federal IT Systems*, June 17, 2005 updates.

5. Phase I—Scope and Core Requirements

The Scope and Core Requirements phase centered on defining an appropriate and reasonable scope for the project. In this step, MITRE examined similar federal programs and systems to review and collect similar Civil Citizens Interactions requirements. By reviewing these other systems business and data requirements, and then selecting a reasonable and representative subset that fits within the defined scope of this program, MITRE could then assemble its baseline business, operations, data, performance, and other core requirements. These requirements then formed the set of requirements used in MITRE's generic baseline Model for this research.

This requirements identified for MITRE's baseline are purposely a set of hybrid requirements to be used only in this research as a reasonable example for proof of concept and as an example for how to apply this process. Phase 1 key goals are as follows:

- **Research Model Scope—**define a high-level scope definition for this research Model
- **Representative Projects Consolidated Core Requirements—**define a generic set of representative project types to be used in this research as assembled from the reprehensive projects reviewed
- **Operating Data Requirements and Impact Summary—**define a generic set of data and impact definitions for this model system.

5.1 Research Model Scope

The scope of this project is to show that a reasonable, operational balance between reasonable security and availability/accessibility to the user can be defined. The goal was to identify a reasonably representative set of data, technical and operational functionality, and systems capacity for this Model. This research then steps through a set of standard NIST processes to identify the level of risks and the corresponding level of required controls and costs. MITRE's core guidelines, as organized by the eight principles of data security [1] [2]and the implications to this research scope, are as follows:

1. **Computer security should support the organization's mission—**security must support the mission but also be balanced against the needs of the citizen and improve service to the citizen for this Model. This drives the design of the solution to be effective, but not overbearing to the end user.
2. **Computer security is an integral element of sound management—**Model seeks to provide a method to assure the organization's management that the proper balance of security and risk has been identified and applied—a process for documenting this balance is critical.
3. **Computer security should be cost-effective—**Cost Benefit Analysis (CBA) must take into account direct and indirect risks and benefits. This research Model will provide a

[1] NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook.

[2] NIST Special Publications 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems

factor to include secondary impacts, beyond the core system and data itself, to the enterprise of security breeches.

4. **System owners have computer security responsibilities outside their own organizations—**users of a system must be made aware of the security capabilities and limitations of the system. Confidence in the system and the perception of a strong security environment is critical for system usage and ultimate success.
5. **Computer security responsibilities and accountability should be made explicit—** scope and boundaries for security responsibilities should be well understood by systems owners/providers and the user community. In this research, MITRE has focused its solution to address vulnerabilities within MITRE's scope of control, provided tools to extend the boundaries when and if possible, and informed the user of user requirements for a reasonable level of security.
6. **Computer security requires a comprehensive and integrated approach—**research will lead to innovative solutions that will require comprehensive and integrated communications and technology effort to the citizen. To be effective, any solution must be supported by a sufficient level of information on the operation of, risks, and responsibilities of the citizen to use the Secure Channel effectively. For example, basic security concepts (e.g., password and authentication procedures) must be well-known by users to be effective.
7. **Computer security should be periodically reassessed—c**itizen user environment is, and will continue to be, a rapidly changing environment. As Citizens move to more advanced and functionally capable mobile devices (e.g., procedures and tools), the risks and threats will have to be constantly reevaluated and assessed.
8. **Computer security is constrained by societal factors—**the Research Team recognizes the challenges of a balance between adequate security and Citizens privacy. The scope of the solutions proposed in this research assume that alternative traditional paper, telephone, in person, or other non-computer channels exist to provide an acceptable redundant channel for interacting with the Citizen. This assumption is critical because the scope of this research, and a core design factor, is that the citizen will always have a choice and be informed before any potentially intrusive data collection is undertaken for account setup, authentication, or placed on the Citizen's system for technology and data security.

Scope will therefore be limited to a reasonable level of technology and required security controls, as appropriate, for the risk defined, the complexity of the mission, and the risk profile assumed by the mission after a review of potential secondary impacts of security weaknesses. The level of security applied will be directly driven by data sensitivity and risk assessments. The model solution outlined in this work will highlight that there is a process for defining and that creative solutions are available for implementing the required security controls and functionality more then proving the absolute scalability or the pilot implementation. Some minimal security policy data collection and enforcement, and the resulting minimal security capability and configuration on the user's computer environment, both will require citizens' cooperation and action if access to the government channel system is desired. Changes to that citizen's computer environment by MITRE's automation, and any risk to the Citizen' systems, is beyond this

researches' scope. Final security certification for a specific use will however be beyond this researches" scope and focus.

5.2 Representative Projects Consolidated Core Requirements Summary

MITRE needed to understand and review a comprehensive list of information items collected, disseminated, or maintained by each generic system type. This list is designed to represent known potential federal application areas. The goal of this list is to assemble and review the group of programs and attempt to represent a reasonable working set of generic data and operational needs in the resulting set of information for MITRE's model. Individually, the collected pieces of data may not appear to be very sensitive, but the information, as a whole and along with other data, may often increase in sensitivity.

Requirements and solutions for federal Civil projects in several Civil agencies were taken into consideration for developing a common criteria and framework. For the propose of this research, these projects and agencies will only be identified generically, with specific information consolidated to prevent any possibility of disclosing sensitive or proprietary information.

5.3 Generic Summary Descriptions of Surveyed Federal Systems with Citizen Interaction Requirements

Federal systems with Citizen Interaction Requirements that were surveyed included the following:

- A Civil Federal Survey Organization
- A Civil Security Organization
- A Citizen payment and collection processing Organization
- A Civil Citizen Web Portal and Publications Organization
- A Civil Benefits Organization
- Other smaller agencies with specific Citizen Interactions as a Core Business.

To preserve sensitive data and information, specific data from existing or proposed federal systems was not directly used in this research. Several representative systems for each type were reviewed and analyzed. Samples of this data set are included in Table 1. A review then resulted in the set of generic systems data requirements and types to define a generic and representative research data Model.

At a minimum, the information listed below was collected on representative projects. This information was then used to define a baseline set of generic requirements and data elements. The resulting dataset from Table 1 that was selected to be used as a baseline included:

- Name—Full name
- Sex—Male or Female
- Address—Full Mailing Address
- DoB—Date of Birth
- PoB—Place of Birth, City and State

- Phone Number
- SSN—Social Security Number
- Email address
- Height
- Weight
- Race
- Marital Status
- Income
- Credit card type
- Account number
- Security Code
- Exp. Date

Table 1. Federal Systems Types and Data Elements

	Generic Federal Survey	Generic Federal Security	Generic Federal Payment/ Collection	Generic Federal Web Portal and Publications	Generic Federal Civil Benefits	Generic "Small" Federal Civil Agency Citizen Interactions
	Name	Name	Name	Name	Name	Name
	Sex	Sex	Title		Sex	Sex
	Address	Address	Address	Address	Address	Address
	DoB	DoB	Phone		DoB	DoB
	Phone	PoB	Item number or count	Item count	PoB	
	SSN	SSN	Item name or description	Item name	SSN	SSN
	Email address	Email address	Email address	Email address	Email address	Email address
	Height	Height	Account holder name		Phone	Phone
	Weight	Weight	Billing address			Billing address
	Race	Race	Credit card type			Credit card type
	Marital status	Port of entry	Account number			Account number
	Income	Date of entry	Security code			Security code
	Type of dwelling	Airlines	Exp. date			Exp. date

	Generic Federal Survey	Generic Federal Security	Generic Federal Payment/ Collection	Generic Federal Web Portal and Publications	Generic Federal Civil Benefits	Generic "Small" Federal Civil Agency Citizen Interactions
	Living status	Country of origin	Routing number			
	Number at household		Check number			
Information disseminated	Only as averages	Yes	No	No	Yes	No
Information maintained	Yes	Yes	Yes	No	Yes	Yes
Information exchanged with other agencies/departments	No	Yes	Yes	Yes	Yes	Yes
Type of authentication used	TBD	Two factor	Two factor	None	Two factor	None
Type of user registration process	Online	Online	Online	Online	Online	Online
Type of remote systems to be supported (e.g., Mac, Windows, UNIX)	All	All	All	All	All	All
Remote system requirements	Yes	Yes	Yes	Yes	Yes	Yes
System availability percentage	100%	100%	100%	95%	100%	90%
System peak period	10am-2pm 6pm–10pm	9am-4am 11pm–4am	10am-2pm 6pm–10pm	10am-2pm 6pm–10pm	10am-2pm 6pm–10pm	10am-2pm
Number of concurrent users supported	10,000	10,000	1,000	TBD	1,000	1,000
Compliance requirements	FISMA	FISMA	FISMA	FISMA	FISMA	FISMA
Sensitivity level	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate

5.4 Operating Data Initial Requirements Analysis and Summary

The operating data was initially analyzed and categorized for design considerations by the following:

- Data Security Level Identification
- Data Security Categorization
- Information Systems Impact Levels

5.4.1 Data Security Level Identification

One of the great challenges for many Civil Agency Secure Citizen Channel applications is in determining a clear, concise, and consistent definition of the data security level in the system. Often internal agency requirements differ greatly in definition and format from Civil agency to agency.

"The long-standing confidentiality-based information classification system for national security information (i.e., CONFIDENTIAL, SECRET, and TOP SECRET) is based only upon the need to protect classified information from unauthorized disclosure; the U.S. Government does not have a similar system for unclassified information. No government-wide schemes (for either classified or unclassified information) exist, which are based on the need to protect the integrity or availability of information."[3]

The Computer Security Act provides a much broader definition of the term "sensitive" information:

> "Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy." [3]

For the purposes of this research, all data will be defined as "sensitive" as stated above. MITRE recognizes that individual agencies may have addition specific requirements; however, MITRE believes this process will work if applied systematically to several situations.

5.4.2 Data Security Categorization

NIST 800-60[4] provides the required process for assigning impact levels and security categorization based on the standards outlined in FIPS 199[5].

"FIPS Publication 199 defines three levels of *potential impact (Low, Moderate, and High)* to organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall national interest."[5]

The process used for mapping data to Security Category for this research Model is taken from NIST 800-60. The initial scope and the core data elements, as defined in Section 2, are used as inputs into the data categorization.

"The security category of an information type can be associated with both user information and system information and can be applicable to information in either electronic or non-electronic form. It can also be used as input in considering the appropriate security category of an information system (see description of security categories for information systems below). Establishing an appropriate security category of an information type essentially requires

[3] NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook

[4] NIST 800-60, Version 2, Guide for Mapping types of Information and information Systems to Security Categories, Volume 1 & 2 , June 2004.

[5] FIPS 199, Standards for Security Categorization Of Federal Information and Information Systems, Feb 2004.

determining the *potential impact* for each security objective associated with the particular information type.

The generalized format for expressing the security category (SC) of an information type is: **SC** information type = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)}, where the acceptable values for potential impact are Low, Moderate, High, or Not Applicable." [6] The data elements used for the research Model can be mapped to data types as defined in NIST 800-60. The selected data elements are all defaulted at this point to be Privacy Act data.

Selected Representative Data Set for this Research included the following:

- Name—Full name
- Address—Full Mailing Address
- DoB—Date of Birth
- PoB—Place of Birth, City and State
- Phone Number
- SSN—Social Security Number
- Email address
- Height
- Weight
- Race
- Marital Status
- Income
- Credit card type
- Account number
- Security Code
- Exp. Date

SC Privacy Act = {(**confidentiality**, Moderate), (**integrity**, Moderate), (**availability**, Low)}

5.4.3 Information System Categorization

"Determining the security category of an information system requires slightly more analysis and must consider the security categories of all information types resident on the information system. For an information system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information resident on the information system."

The generalized format for expressing the security category, **SC**, of an information system is:

SC information system = {(**confidentiality,** *impact*), (**integrity,** *impact*), (**availability,** *impact*)}, where the acceptable values for potential impact are Low, Moderate, or High."[6] The data elements used

[6] FIPS 199, Standards for Security Categorization Of Federal Information and Information Systems, Feb 2004

for the research Model can be mapped to Mission-based Information types as defined in NIST 800-60[7].

i. A Civil Federal Survey Organization

Mission Type: SC General Purpose Data and Statistics Information ={(**confidentiality,** *Moderate*), (**integrity,** *Low*), (availability**,** *Low*)},

A Civil Security Organization

Mission Type: SC Border Control and Transportation Security ={(**confidentiality,** *Moderate*), (**integrity,** *Moderate*), (availability**,** *Moderate*)},

ii. A Citizen Payment and Collection Processing Organization

Mission Type: SC Debt Collection Information = {(confidentiality, *Moderate*), (integrity, *Low*), (availability, *Low*)},

iii. A Civil Citizen Web Portal and Publications Organization

Mission Type: SC Product Outreach Information={(confidentiality, *Low*), (integrity, *Moderate*), (availability, *Low*)},

iv. A Civil Benefits Organization

Mission Type: SC Benefits Management Information= {(confidentiality, *Moderate*), (integrity, *Low*), (availability, *Low*)},

Federal Systems Types and Data Elements Mission Type: SC Personal Identity and Authentication Information = {(**confidentiality,** *Moderate*), (**integrity,** *Moderate*), (**availability,** *Moderate*)},

"FIPS Publication 199 requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The potential impact values assigned to the respective security objectives are the highest values (i.e., high water mark) from among the security categories that have been determined for each type of information resident on those information systems."[8]

Summary, "water mark" **SC** for the **Research Model** = {(**confidentiality,** *Moderate*), (**integrity,** *Moderate*), (**availability,** *Moderate*)},

[7] NIST 800-60, Volume II: Appendixes to Guide the mapping Types of Information and Information Systems to Security Categories, June 2004

[8] FIPS 200, Minimum Security Controls for Federal information Systems, Fall 2005

6. Phase 2—Define Baseline Investigation Model

Phase 2 defines the details of the baseline Model for this effort. For this research, it is defined as a "Model" because it is meant to be a generic set of assembled requirements, specifications, and operating parameters from similar Civil agencies. This generic set was used and then the overall process outlined in this research was applied to it. In a specific systems implementation, this "Model" would be replaced by the requirements for the specific Citizens Interaction Channel being deployed.

For this research, a hybrid set of functions was created to represent a generic federal Web-based system. The specific business requirements and functions are less critical then the general Citizen Web Interaction capability and the function and types of data involved. Based on the analysis in the previous section, an information system and a set of data types with a "Moderate" security classification level is a requirement. This baseline Model will therefore specify a system with a "Moderate" security classification and confidentiality, integrity and availability levels at "Moderate," as well.

The web-based Citizen Portal defined below is therefore not representative of any one specific federal function; it instead combines several independent "federal" functions and data types into one "Model" system for the evaluation of security concepts vs. pure business function. This "System" Model will be the foundation for the Data Sensitivity Risk Assessment and the traditional NIST 800-53 and NIST 800-53A-based security risk assessment. These assessments will be integral phases and will drive the final Model system design and configuration phases to the final level of detail for the pilot implementation and demonstration system.

6.1 Generic Business Operations

High-level Functional System Overview—generic federal agency was defined with a mission of tracking a segment of the Citizenship for a benefit distribution function. This generic agency's mission includes the following key mission elements:

- Maintaining a Citizen database of potential Citizen beneficiaries
- Updating this database with the latest contact and required Citizen information to calculate benefit qualifications activation dates, and current contact information for that Citizen
- Processing annual information gathering efforts to update its statistical data on this segment of the population
- Offering supplemental and third-party documentation for a minimal fee

Presentation—information display segmented into five screen presentations:

1. Authentication and Login—OMB 06-169 requires two-factor authentication for all Moderate and above security categories
2. Registration and User Profile Updates—capability required to register users and allow users to update their profile information.

[9] OMB 06-16 Protection of Sensitive Agency Information, June 23, 2006

3. Survey Collection—capability required to allow the government agency to collect selected survey information from the Citizen in a secure environment. The Citizen must be fully informed of the nature of this data collection, the use of the data, and the security implemented
4. Purchase Selection—capability required to allow the Citizen to select a document for purchase
5. Payment—capability required to allow the Citizen to securely pay for the purchase with a credit card

User Interaction—user interaction opportunities will map to the presentation and required business functions**:**

- Registration
- Account edits and user profile updates
- Data collection
- Product selection and payment

Data Processing—data retention and background processing will be as follows:

- Citizen Identification, Authentication, and Other Profile information—any required state data to allow these processes to function and to maintain basic Citizen user data
- Survey Data Storage—secure storage for the collected Citizen Survey information
- Product Control—control and tracking of products offered for purchase
- Product Delivery Status—status of products delivered to the Citizen
- Customer Service/Payment Information—information to allow the secure completion of the Citizen's purchase payments

User Environment—target user environment would be inclusive of a majority of the "mainstream" Citizen systems in current usage and available vender support to the Citizen.

- User Access Channels
  - Home and other unsecured PC platforms—target hardware environment for the Citizen is a private PC; however, the Citizen may attempt to access the system through a public internet terminal hosted on a PC. Mobile device access is also a viable channel consideration and MITRE will include it as a consideration in its review
  - Broadband and dialup internet—Model will not have dependence on the type or speed of connecting the internet channel for Citizen access
- User Platforms Supported
  - Windows, XP (SP4 and above), and Vista
  - Apple OS
  - Linux OS

Capacity and Performance—core design would be representative of a "real world" federal system. The design parameters listed below are for this "generic," "real world" federal environment.

- Concurrent users—system must support at least 1,000 concurrent users and a total projected user community of one million users. (The Pilot system outlined as a demonstration will be designed for this research as a proof of concept to highlight the availability and potential of existing and new technologies. Therefore, the Research Pilot system will support a minimal demonstration capacity for concurrent users, data storage, and availability.)
- System response—system must respond to user input within five seconds.
- System availability—system must be available 99 percent during normal business hours.
- System storage—system must have data storage available for one million users.

6.2 Baseline Model Data, Technical, and Functional Architectures

The goal of this research is to identify capabilities and weaknesses and then attempt to address any weaknesses using standard available federal guidelines, processes, and requirements. The data and technical architecture are representative of generic Citizen Channel requirements as outlined in this research.

Baseline Data Architecture

The generic representative data field elements that were selected are listed below:

- Name—Full Name
- Address—Full Mailing Address
- DoB—Date of Birth
- PoB—Place of Birth, City and State
- Phone Number
- SSN—Social Security Number
- Email Address
- Height
- Weight
- Race
- Marital Status
- Income
- Credit Card Type
- Account Number
- Security Code—Credit Card Security Code
- Card Expiration Date

Data Structures

The data will be structured into three linked data areas:

1. User Registration Data
   – Name—Full name

- Address—Full Mailing Address
- Phone Number
- SSN—Social Security Number
- Email Address

2. User Survey Data
   - Name—Full name
   - DoB—Date of Birth
   - PoB—Place of Birth, City and State
   - SSN—Social Security Number
   - Height
   - Weight
   - Race
   - Marital Status
   - Income
3. User Order and Payment Data
   - Name—Full name
   - Address—Full Mailing Address
   - DoB—Date of Birth
   - PoB—Place of Birth, City and State
   - Phone Number
   - Email address
   - Item ID
   - Credit card type
   - Account number
   - Security Code—Credit Card Security Code
   - Card Expiration Date

Baseline Technical Architecture

The Secure Citizen Notional Model is outlined in Figure 2. The purpose of the Secure Citizen Laboratory demonstrations is to highlight potential technologies that can be effective in delivering government IS services to various client populations.

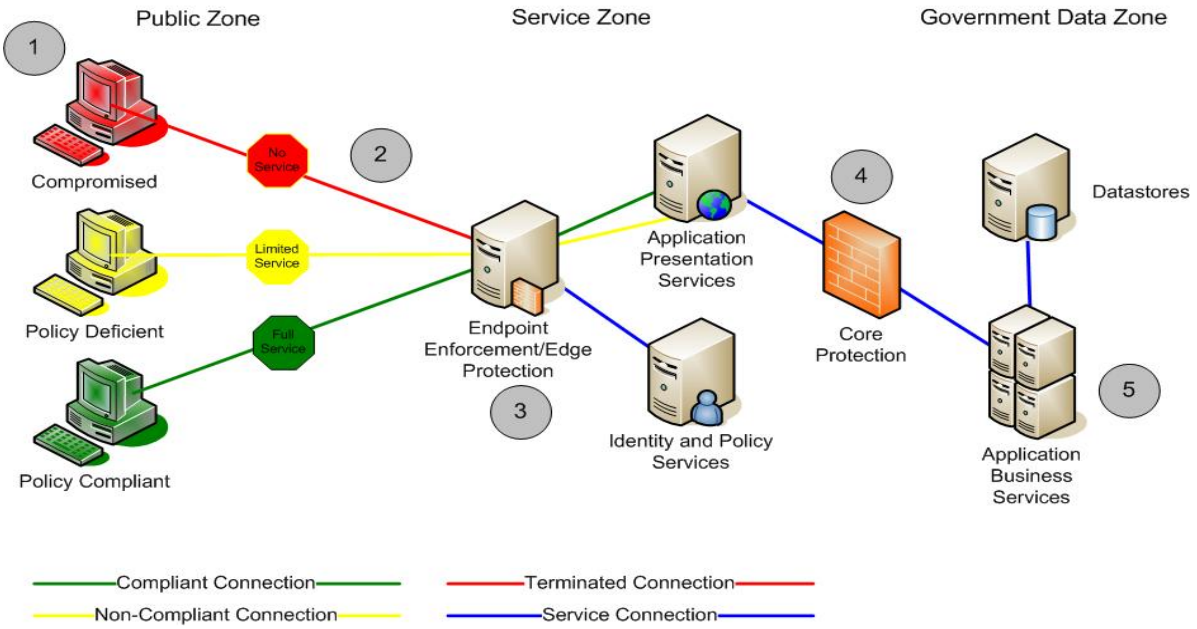

Figure 2. Secure Citizen Interaction Baseline Technology Model

The target is to investigate a multi-tier, web-enabled application environment that is similar to the normal architecture for most modern government client interactions. The goal of the multi-tier laboratory is to take advantage of observing a "near real" environment when controlling network admission and authentication for the Citizen, as well as protecting from insider threat.

Baseline Functional Architecture

The following section addresses the numbered sections of the Secure Citizen Notional Model outlined in Figure 2. It describes the order of operations. Each area is a focus point for the exploration of either technology integration or vendor innovation in the area listed. In this research demonstration, the team focused heavily in the "Number 3" area of policy enforcement and identity management services, which is due to the relatively new innovations in this area in both policy services and post network admission technologies.

1 **Public Zone Simulation—**area simulates various security configurations of a citizen attempting to access a federal government system. The areas of configuration are defined as follows:

1) Policy Compliant—all patches, protection software, and updated vulnerability profiles are up-to-date. This citizen computer has a better than average expectation of interacting securely with the government without a mandated update or change to its core system features.

2) Policy Deficient—at least one factor of the system has become a threat to compliance and thus the simulation will look to measure how well the next policy enforcement tier will react to the possible connection.

3) Compromised—after an initial scan, this citizen is found to have an exploited vulnerability and should never be connected to the Secure Client network.

2 **Service Determination—**section is literally where the data translates to policy and the area where the citizen's posture is first checked against the known rules as delivered by the policy services. Service determination will be based upon several criteria, including patch level, operating system (OS) instrumentation discovery, and network traversal.

3 **Endpoint/Edge Enforcement—**set of services that is at the heart of working to determine if the Citizen is allowed to connect, what the citizen is allowed to connect to, and at what level of security posture the citizen is vetted into. This service constitutes the most "cutting edge" of all the technologies MITRE will evaluate, as it is an up-and-coming pattern that fills a real need when allowing network admission to evaluate a client and recommend updates prior to access.

4 **Core Protection—**core protection service is the internal firewall portion of the environment. Its purpose is to filter all information about operations and feed it intelligently to security operations staff so the staff can adjust access to the core data stores accordingly

5 **Core Services—**area represents the business rules and the data that is essential to performing day-to-day operations. This service is usually located where internal servers carrying PII or other sensitive data reside.

Network Edge and Core Protection Services

The Secure Citizen Team will use a combination of virtual local area network (VLAN) techniques, combined with SOHO firewalls, to simulate multiple tiers of protocol control and inspection.

Demonstration Concept

The concept of the demonstration is to illustrate technologies that have the potential to break current barriers to network admission control and flexible authentication of large, diverse user population. The last three to five years within the federal government have seen dramatic changes in requirements for agencies to enable interaction with Citizens via public networks (i.e., internet). The federal e-Gov initiative has spawned several initiatives for public services and has also driven standards initiatives, such as Federal E-Authentication. Along with these initiatives are security problems associated with connecting a system that stores and services personal information with a public-facing network. Privacy therefore has become a paramount concern with the ever-increasing threat of identity theft, as well as the relative expertise of the criminals who look to exploit any security weakness for profit. In addition, confirmation of minimal Citizen Host PC configurations is an emerging concern.

Network Endpoint Control

The Secure Citizen Interaction demonstration showcase ways an endpoint enforcement system will react when faced with changes of the endpoint system state. These systems states, combined with the variation in platform, illustrate the current state-of-the-art in network admission

technology. In addition, the demonstration uses new and innovative alternative multi-factor authentication mechanisms.

The traditional concept of Network Admission Control (NAC) technology is to allow access to the network resource if all criteria are met by the endpoint host requesting access. If one factor within the policy profile of the network admission control process is not met, then the host is denied access. Within organizations that have a managed desktop environment, this is a practical possibility because the organization controls the endpoint host via a standard deployment and has the ability to sustain patch levels, updates, and other host configuration. Therefore, the two system states that are generally accepted in a traditional NAC are the system either complies or does not comply with the policy and is considered compromised.

In order to meet the needs of the Citizen at large, the infrastructure will still have to use network admission criteria; however, these criteria will have to be tied to tiered levels of access based upon the relative posture of the host requesting access. The public connectivity, as well as those of closer state and local users, will require the NAC toolset to be able to meet a third state. The introduction of a state, where the policy is met to a level of limited access, is necessary to allow users to access certain data and services without a system change on their part, but not have access to the full services of the federal system without moving to compliance with the organization's policy. This state will be called "policy deficient" for the sake of this research activity.

In Summary, there are three possible states that are explored during lab demonstrations:

1. **Policy Compliant**—endpoint requesting access complies with all policies defined by the organization's NAC Program. There are no patches, updates, or additional software needed to satisfy security and privacy controls for access.
2. **Policy Deficient—**state where at least one, but not all, of the policy items are either deficient or cannot be determined by the current network admission control device. There are changes that need to be made to the system to maintain full compliance. Until the user has made the changes, limited access will be granted.
3. **Compromised—**state within where a known control has been compromised on the host requesting access, therefore it cannot be allowed any type of access without remediation.

Secure Citizen Interaction demonstrations probe the issue that the vast majority of public access to federal systems falls into an initial "policy deficient" state and that blanket denial of access will not be practical to ensure that Citizens may interact at a nominal level for some self-service applications. The system demonstration show possible ways to allow for nominal, controlled access, while a Citizen is given the opportunity to become policy compliant.

Currently, the Secure Citizen platform is exploring cutting-edge network admission and policy enforcement mechanisms. One partner, Insightix Corporation, has partnered with MITRE to research the feasibility of the "dissolvable agent" technology. This technology will allow the use of any computing platform by the Citizen, as well as the establishment of a cross platform security baseline, that can be fused to the common risk models mentioned in prior sections of this document.

Flexible Authentication Mechanisms

Flexible Authentication Mechanisms is another primary area of demonstration that allows for multiple levels of user authentication with a variety of factor combinations. Factors for this activity will be defined traditionally as follows:

- What you have—a token or some type of device that can be possessed in order to verify the authenticity of the user
- What you are—use of the user's physical characteristics to authenticate
- What you know—use of knowledge-based activities to authenticate a user

Changes to privacy regulations governing access to personal data within government systems have resulted in the mandate for the use of a second authenticity factor beyond the standard username and password ("what you know") to combine with either "what you have" or "what you are." These requirements have created another challenge for Secure Citizen in that the delivery of a second factor to large populations has not yet been attempted for an extremely large or diverse user population.

Many technologies that provide token-based authentication are cost prohibitive for large populations due to user provisioning and deployment issues, as well as the management of the devices and complex technologies that sometimes accompany these devices. Using biometric data with the public is somewhat impractical because of privacy concerns, as well as the relative reliability of current technology.

These factors have forced many vendors to look toward non-traditional second factors in their product offerings, which is an effort to satisfy the need for large populations without the cost of large-scale deployment. These technologies look to leverage devices a user possesses or to deploy very low-cost, disposable tokens that can be easily deployed.

The Secure Citizen Interaction demonstration will focus on the use of a telephone-based authentication system that will allow users to use a pre-registered phone or a cellular phone's SIM identifier to provide the second access factor to the federal system.

Secure Citizen Interaction has partnered with StrikeForce Corporation and Entrust Corporation to study tokenless authentication factors. These tokenless factors can be derived from items already in the Citizens' possession (e.g., cellular telephones, Personal Digital Assistants [PDA], and even a home phone). StrikeForce has provided its "ProtectID" product and Entrust has provided "Identity Guard" for the purpose of this study. The StrikeForce system has a cellular telephone "out-of-band" authentication technology that provides isolation of the requesting system from the credential granting system. Entrust has provided its product that performs multiple levels of authentication from full tokens and Public Key Infrastructure (PKI)-based smart cards to methods as simple as "grid card" technologies, which are easily deployable and at a low cost.

7. Phase 3—Privacy Impact and Data Sensitivity Assessment

Phase 3 has two primary steps. The first step was to perform specific privacy impact and sensitivity assessments to confirm the initial design assumptions outlined previously in this text for this research Model. For this Model, all data types were initially assumed to have a Moderate security classification; however, a review of this privacy and sensitivity level assumption was required.

In this first step, the primary assumption reviewed that all data elements in this research baseline are governed by the privacy provisions of the E-Government Act of 2002.[10] The E-Government Act supplements the requirements in the Privacy Act of 1974. The E-Government Act requires agencies to conduct a Privacy Impact Assessment (PIA) before doing the following:

- Developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public, or
- Initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for ten or more persons (excluding agencies, instrumentalities, or employees of the federal government).

The second step of this phase is to review the FIPS 199 categorization of the data as outlined earlier in this research and the overall system's sensitivity categorization in this context. This step provides additional verification that the information categorization adequately ensures the identification of personally identifiable information requiring protection.

The intent is also to ensure all personally identifiable information through which a moderate or high impact might result has been explicitly identified. For example, databases where loss, corruption, or unauthorized access to Personally Identifiable Information (PII) contained in the databases could result in a serious adverse effect with widespread impact on individual privacy being one area of specific concern.[11]

7.1 Reference Guidelines and Government Standards

MITRE reviewed several publications and requirements to define the required processes, including:

- OMB M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*[12], Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36) requires that OMB issue guidance to agencies on implementing the privacy provisions of the E-Government Act As well as for a description of requirements to conduct a PIA.
- NIST 800-12 for a definition of Sensitivity and a Sensitivity Assessment[13]
- NIST SP 800-53 controls and specific SP 800-53A assessment procedures for the following:

[10] E-Government Act of 2002, signed by the President on December 17, 2002 and became effective on April 17, 2003

[11] OMB M-06-16 Protection of Sensitive Agency Information, June 23, 2006

[12] OMB M-03-22 , OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003

[13] NIST 800-12, An Introduction to Computer Security, The NIST Handbook

- Privacy Impact Assessment (PL-5)
- Security Categorization (RA-2)

7.2 Privacy and Sensitivity Assessment Definitions

PIA Definition:

OMB gives guidance in OMB 03-22[14] and defines a PIA as:

> "An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks."

Sensitivity Assessment Definition:

The NIST Security Handbook, NIST 800-12[15] defines Sensitivity as:

> "The definition of sensitive is often misconstrued. Sensitive is synonymous with important or valuable. Some data is sensitive because it must be kept confidential. Much more data, however, is sensitive because its integrity or availability must be assured. The Computer Security Act and OMB Circular A-130 clearly state that information is sensitive if its unauthorized disclosure, modification (i.e., loss of integrity), or unavailability would harm the agency. In general, the more important a system is to the mission of the agency, the more sensitive it is."

NIST 800-53 and 800-53A both refer to the base definitions for Security Category and Impact assessment in FIPS 199 and in OMB 03-22 as standards.

7.3 Methodology

OMB 03-22 states that a PIA must analyze and describe:

- What information is to be collected (e.g., nature and source)?
  - The information to be collected is Privacy Act level data as defined in section 5.1 above. The information will be sourced from individual Citizens with their consent.
- Why the information is being collected (e.g., to determine eligibility)?
  - To provide statistical information to the government, to provide benefits delivery and product delivery to the Citizen.
- What is the intended use of the information (e.g., to verify existing data)?
  - To provide statistical information to the government, to provide benefits delivery and product delivery to the Citizen.
- With whom the information will be shared (e.g., another agency for a specified programmatic purpose)?

[14] OMB M-03-22 , OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003

[15] NIST 800-12, An Introduction to Computer security, The NIST Handbook

  - Privacy Act and other specific Citizen data will not be shared with OGAs except in statistical summary format. No Citizen specific data will be shared with OGAs.

- What opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?
  - To provide statistical information to the government, to provide benefits delivery and product delivery to the Citizen.
- How the information will be secured (e.g., administrative and technological controls)?
  - The information will be secured as outlined per NIST 800-53 requirements as outlined in the "Security Risk Assessment" Section 8, Phase 4 of this research.
- Whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a.?
  - Per the definition of the Privacy Act of 1974, 5 U. S. C. 552a, a Systems of records is being created and this data must fall under the restrictions and guidelines associated with Privacy Act data.
- PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA.
  - The data remained at a Moderate level of Security Categorization after this review.

NIST 800-12 states that a sensitivity assessment should answer the following questions:

- What information is handled by the system?
  - The information to be collected is Privacy Act level data as defined in Section 5.1. The information will be sourced from individual Citizens with their consent.
- What kind of potential damage could occur through error, unauthorized disclosure, modification, or data unavailability of the system?
  - The information to be collected is Privacy Act level data as defined in Section 5.1. The exposure to potential impact for a Moderate security objective for confidentiality, integrity and availability is defined as "serious" for the proposed data and system functionality as defined in FIPS 199. FIPS 199 further defines a *serious* adverse effect on organizational operations, organizational assets, or individuals as

    A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.[16]
- What laws or regulations affect security (e.g., Privacy Act or Fair Trade Practices Act)?
  - Privacy Act data is assumed.
- To what threats is the system or information particularly vulnerable?

[16] Note: The secondary impacts would be specific to a particular application, function and agency and would be documented in more detail then is possible for this research model.

– This "Threat Assessment" section describes the major threats against which this Secure Citizen Interaction Channel must be defended.

An abstract view of the channel is shown in Figure 3. It consists of a (1) computer used by the Citizen to interact with the government system, (2) a government system, (3) a firewall protecting the government system from external network penetration, (4) an internet connection between the Citizen's computer and the firewall, and (5) a private connection between the firewall and the government system. This research is primarily concerned with threats against system parts that include the Citizen's computer, the internet, and the firewall; there are additional threats that apply to the greater system, but as these exist regardless of how data enters the system, they are outside the scope of this research.

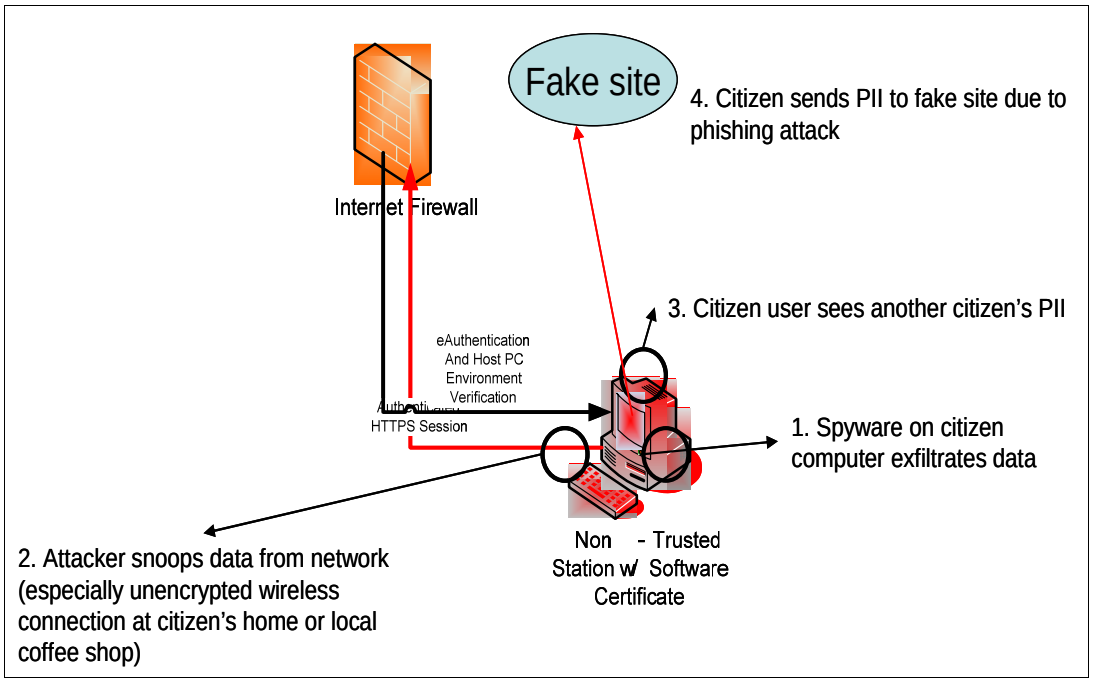

Figure 3. Abstract Channel View

MITRE's analysis illustrates the following major threats to the information being provided by Citizens to the government system:

1. The security of the Citizen's computer is unknown, thus MITRE assumes it has been compromised; therefore, it could contain spyware that can exfiltrate data that is transmitted to or from the government system, which passes through the Citizen's computer. It can easily do this without the knowledge of the Citizen.
2. Data transmitted over the channel could be read by an attacker while it is in transit. While it is common for data transmittals to take place over an encrypted network session, making it very difficult for someone besides the Citizen and the government to read, data is very often sent in plain text over unencrypted network connections. As Citizens increasingly use unencrypted wireless connections from home and in public areas (e.g., coffee shops) instead of hardwired connections at

home, the opportunities for attackers to read data while in transit over the network has increased.

3. If the government system is incorrectly programmed, it is probable that one Citizen may inadvertently see another Citizen's data. While this data may simply confuse the first Citizen (who expects to see only his data), it is not possible to rule out data misuse.
4. A Citizen may intend to supply his personal information to the government, but may instead provide it to a rogue or fake site due to a social engineering attack, such as phishing.[17] In this case, the government never obtains the information, but the Citizen believes he has provided it to the government.

These threats are in addition to any that are possible against the government system if that system is set up only to allow data access by government employees from behind the firewall. The defenses in this case, briefly, are:

1. The government can control the configuration of the computers used to access the data. It can run spyware detection and removal tools on the computers, as well as reduce the opportunities for spyware to be put on the computers in the first place.
2. The government can control the connections between its computers and the data by enforcing encryption at all times, for instance. Further, it controls and limits access to the network itself behind the firewall.
3. By limiting access to system data to government employees, the government can limit the possible damage in the event that an employee sees data the employee should not see. Employees may be screened to increase assurances of their reliability, and they may be subjected to policies if they violate the trust inherent in their position.
4. Government users would be unlikely to access an internal system by way of a link in an email. Also very easy to flag, when a user is going from inside to outside of the firewall to access a system, and the user could be alerted or the connection could be blocked.

– In summary, adding Citizen access to government systems from the internet increases the number of threats to Personally Identifiable Information (PII) because of the lack of control the government has over the Citizen's computer configuration. As part of this control, the proper identification and authentication of this Citizen is required to control access and to allow these defenses to function.

No threats were identified in excess of those for an equivalent commercial Web application.

- Are there significant environmental considerations (e.g., hazardous location of system)?
  – None assumed in excess of those for an equivalent commercial Web application.
- What are the security-relevant characteristics of the user community (e.g., level of technical sophistication and training or security clearances)?

[17] Phishing refers to having the Citizen use his internet browser to view a link to a rogue site provided in an email which masquerades as being legitimately from the government. The end result is to provide the Citizen's information to the attacker, as with the spyware threat, though in the case of phishing, no special software from the attacker is required.

  - No classified data will be processed. No other special characteristics were assumed in excess of those for an equivalent commercial Web application.
- What internal security standards, regulations, or guidelines apply to this system?
  - No agency specific additional security requirements are assumed in excess of those required for a federal Web application.

NIST 800-53 and 800-53A require that:

- Privacy Impact Assessment (PL-5.1)

  (i) The organization conducts a privacy impact assessment on the information system in accordance with OMB policy

  (ii) The privacy impact assessment is consistent with federal legislation and OMB policy.
- Security Categorization (RA-2)

  (i) the organization conducts the security categorization of the information system as an enterprise-wide exercise with the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and mission/information owners;
- This research assumes this coordination would occur in the Agency.

  (ii) The security categorization is consistent with FIPS 199 and NIST SP 800-60

  (iii) The organization considers in the security categorization of the information system, potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001, and Homeland Security Presidential Directives, potential national-level impacts
- No impact for or due to the system and data type assumed and used in this research for a generic Federal Civil Agency system.

  (iv) The organization includes supporting rationale for impact-level decisions as part of the security categorization
- This research assumes that isolated situations of Privacy data loss could have an impact on the agency in a potential Citizen loss of confidence and reductions in systems utilization. This could in turn reduce the data collection; however, after extensive review of the FIPS 199 and FIPS 200 definitions on impact level and severity, this research still concluded the Security classification should be Moderate for this Model.

  (v) Designated, senior-level organizational officials review and approve the security categorization of the information system.
- This research assumes this coordination would occur in the Agency.

7.4 Summary of Sensitivity Assessment Results for this Model

In summary, the data classification for the research Model and its associated data remains at the M**oderate level**. All data was conservatively classified as **Privacy Act Data** and this will be the basis for the design and the Security Risk Assessment.

8. Phase 4—Security Risk Assessment

Phase 4 maps the appropriate NIST 800-53 800-53A guidelines to the definition, design, and security controls of the baseline Model for this research. This review of the Model design and requirements against the guidelines, processes, and requirements also considered other appropriate references cited in Section 4 and documented in this section.

8.1 Security Risk Assessment Definition

Risk management encompasses three processes: (1) risk assessment, (2) risk mitigation, and (3) evaluation/assessment. Risk Management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions. Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its lifecycle. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.[18]

For this research, the Security Risk Assessment component will focus on a mapping of Secure Citizen Channel Model characteristics to the NIST 800-53 Security control matrix. By comparing MITRE's baseline design to the requirements for a Moderate system level, MITRE will be able to map its model's capabilities, highlight areas where additional controls may be required, and highlight where current technology shows areas of concern.

Thus, for this research, the Security Risk Assessment is defined as the process of mapping Model's known level of functionality and baseline systems design to the available security controls. As part of this assessment consideration, an analysis of key threats to the type of system was also considered.

8.2 Reference Guidelines and Government Standards

The Guidelines and government standards baseline for this research Model are based on the Federal Information Security Management Act (FISMA) of 2002, P.L. 1107-347. Key Risk Assessment related documents are:

- FIPS 199, *Standards for security Classification of Federal Information and information Systems*
- FIPS 200, *Minimal Security requirements for Federal Information and information Systems*
- NIST 800-53 *Recommended Security Controls for Federal information Systems*, February 2005
- NIST 800-53 *A Guide for Assessing the Security Controls in Federal Systems*, June 2007

This work is also consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-

[18] NIST 800-30, Risk Management guide for Information Technology Systems, July 2002

130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in A-130, Appendix III.

8.3 Methodology

The initial inventory and controls applied to the Model for this research is included in Table 2.

Table 2. Security Requirements and Control Mapping

CNTL NO.	Control Name	"Moderate" 800-53A Requirements	Model Proposed Implementation/ Control
		Access Control	
AC-1	Access Control Policy and Procedures	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and developing policy and procedure is considered out of scope.
AC-2	Account Management	AC-2 (1) (2) (3)	A directory will be used to store all user accounts and associate users with groups, based on access rights/privileges.
AC-3	Access Enforcement	AC-3 (1)	The identity and policy services component will provide the ability to create access control policies to control access between users and objects.
AC-4	Information Flow Enforcement	AC-4	Policies created in the identity and policy services component will provide a degree of flow control. The applications business services themselves can be designed to regulate where information is allowed to travel.
AC-5	Separation of Duties	AC-5	Administration, monitoring, user provisioning, and application support and development tasks will be split amongst different organizations within and agency. All parts of the system support access controls to enforce this separation of duties. This control is not relevant for the purposes of this Model.
AC-6	Least Privilege	AC-6	Access controls will be configured to enforce the most restrictive set of rights needed by users.
AC-7	Unsuccessful Login Attempts	AC-7	The identity and policy services component will enforce a limit of consecutive invalid access attempts by a user over a specified period of time.
AC-8	System Use Notification	AC-8	Application presentation services will display a message to all users informing them that they are accessing a government system, they are being monitored, unauthorized use is prohibited, and using the system indicates consent to monitoring.
AC-9	Previous Logon Notification	AC-9	Application presentation services will notify a successfully logged on user of the time and date of the last logon attempt and number of any unsuccessful logon attempts.
AC-10	Concurrent Session Control	AC-10	Applications services will be designed to limit a user to a single concurrent session.

CNTL NO.	Control Name	"Moderate" 800-53A Requirements	Model Proposed Implementation/ Control
AC-11	Session Lock	AC-11	Application services will prevent further access to the system after a period of user inactivity.
AC-12	Session Termination	AC-12	Application services will terminate remote session after a longer period of inactivity.
AC-13	Supervision and Review—Access Control	AC-13	All components of the Model will support detailed logging of user access and privilege use.
AC-14	Permitted Actions w/o Identification or Authentication	AC-14 (1)	An agency will identify any specific user actions that are permitted without identification or authentication. The application can be designed to support this. Only general information will be provided without authentication for this Model.
AC-15	Automated Marking	Not Selected	The application will mark system output with handling instructions for any PII. The Model will not implement this control, as it is not relevant to the objective.
AC-16	Automated Labeling	Not Selected	Data contained in the system will be labeled to indicate access control requirements or special dissemination requirements. The Model will not implement this control, as it is not relevant to the objectives.
AC-17	Remote Access	AC-17 (1) (2) (3)	The Model target user populations will all be accessing applications remotely. The endpoint enforcement/edge protection component will monitor and help control remote access to applications. Cryptography will be used between users and this system.
AC-18	Wireless Access Restrictions	AC-18 (1)	None of the Model components will make use of wireless technology. It is possible end-users may, so end-to-end encryption will be required for application access.
AC-19	Access Control for Portable and Mobile Systems	AC-19	The endpoint enforcement component will attempt to validate the security posture of end user's systems, prior to allowing access. This is possible by using dissolvable agents to scan users' systems to identify noncompliance with minimal acceptable configuration and potentially compromised system.
AC-20	Personally Owned Information Systems	AC-20	External (non-government owned) systems will need to access the Model application. Agencies must set terms and conditions for users to access applications and handle information exposed by the system. The endpoint enforcement component can verify the use of required security controls on these external systems.
Awareness and Training			
AT-1	Security Awareness and Training Policy and Procedures	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and developing policy and procedure is considered out of scope.
AT-2	Security Awareness	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and conducting awareness training is considered out

CNTL NO.	Control Name	"Moderate" 800-53A Requirements	Model Proposed Implementation/ Control
			of scope.
AT-3	Security Training	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and conducting awareness training is considered out of scope.
AT-4	Security Training Records	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and conducting awareness training is considered out of scope.
Audit and Accountability			
AU-1	Audit and Accountability Policy and Procedures	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and developing policy and procedure is considered out of scope.
AU-2	Auditable Events	AU-2	Various components of the Model will support granular auditing of events of interest.
AU-3	Content of Audit Records	AU-3 (1)	Various components of the Model will support granular auditing of events of interest, listing a timestamp, component, and type of even.
AU-4	Audit Storage Capacity	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and storage capacity for audit logs will not be an issue with this Model.
AU-5	Response to Audit Processing Failures	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and hardware or software failures with the auditing system will not be evaluated.
AU-6	Audit Monitoring, Analysis, and Reporting	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and audit reporting is considered out of scope.
AU-7	Audit Reduction and Report Generation	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and audit reporting is considered out of scope.
AU-8	Time Stamps	AU-8	Time stamps will be part of all audit events generated by components of this Model.
AU-9	Protection of Audit Information	AU-9	Access controls will be applied to all audit information generated by components of this Model.
AU-10	Non-repudiation	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and non-repudiation of audit information is considered out of scope.
AU-11	Audit Retention	AU-11	Audit logs will be retained, but this control is more relevant for an operational system.
Certification, Accreditation, and Security Assessments			
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and developing policy and procedure is considered out of scope.
CA-2	Security Assessments	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and

CNTL NO.	Control Name	"Moderate" 800-53A Requirements	Model Proposed Implementation/ Control
			security certification, accreditation and assessment activities are considered out of scope.
CA-3	Information System Connections	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and security certification, accreditation and assessment activities are considered out of scope.
CA-4	Security Certification	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and security certification, accreditation and assessment activities are considered out of scope.
CA-5	Plan of Action and Milestones	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and security certification, accreditation and assessment activities are considered out of scope.
CA-6	Security Accreditation	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and security certification, accreditation and assessment activities are considered out of scope.
CA-7	Continuous Monitoring	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and security certification, accreditation and assessment activities are considered out of scope.
Configuration Management			
CM-1	Configuration Management Policy and Procedures	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and developing policy and procedure is considered out of scope.
CM-2	Baseline Configuration	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and configuration management activities are considered out of scope.
CM-3	Configuration Change Control	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and change control activities are considered out of scope.
CM-4	Monitoring Configuration Changes	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and configuration management activities are considered out of scope.
CM-5	Access Restrictions for Change	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and change control activities are considered out of scope.
CM-6	Configuration Settings	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and configuration management activities are considered out of scope.

CNTL NO.	Control Name	"Moderate" 800-53A Requirements	Model Proposed Implementation/ Control
CM-7	Least Functionality	CM-7	Only essential capabilities will be enabled on components of this Model.
Contingency Planning			
CP-1	Contingency Planning Policy and Procedures	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and developing policy and procedure is considered out of scope.
CP-2	Contingency Plan	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and contingency planning is considered out of scope.
CP-3	Contingency Training	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and contingency planning is considered out of scope.
CP-4	Contingency Plan Testing	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and contingency planning is considered out of scope.
CP-5	Contingency Plan Update	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and contingency planning is considered out of scope.
CP-6	Alternate Storage Sites	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and contingency planning is considered out of scope.
CP-7	Alternate Processing Sites	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and contingency planning is considered out of scope.
CP-8	Telecommunications Services	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and contingency planning is considered out of scope.
CP-9	Information System Backup	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and contingency planning is considered out of scope.
CP-10	Information System Recovery and Reconstitution	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and contingency planning is considered out of scope.
Identification and Authentication			
IA-1	Identification and Authentication Policy and Procedures	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and developing policy and procedure is considered out of scope.
IA-2	User Identification and Authentication	IA-2	A risk assessment (OMB 04-04) will likely conclude this Model to be a level 3 system. Based on requirements specified in NIST 800-63 and OMB 06-16, multifactor authentication will be required and implemented for user authentication and access to the application services.
IA-3	Device Identification and Authentication	IA-3	The endpoint provisioning component will have the ability to uniquely identify specific devices, before they are permitted to establish a connection
IA-4	Identifier Management	IA-4	Users account provisioning will be discussed in this document and it will be supported in the Model to a degree, but it is outside the scope of

CNTL NO.	Control Name	"Moderate" 800-53A Requirements	Model Proposed Implementation/ Control
			this work to document and build a complete user provisioning system as part of this Model.
IA-5	Authenticator Management	IA-5	Authenticator provisioning will be discussed and solutions will be demonstrated that can enable this control for the diverse use population given.
IA-6	Authenticator Feedback	IA-6	The feedback of authentication information will be masked, during the authentication process.
IA-7	Cryptographic Module Authentication	IA-7	Components used in this Model will be FIPS 140-2 compliant.
Incident Response			
IR-1	Incident Response Policy and Procedures	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and developing policy and procedure is considered out of scope.
IR-2	Incident Response Training	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and incident response is considered out of scope.
IR-3	Incident Response Testing	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and incident response is considered out of scope.
IR-4	Incident Handling	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and incident response is considered out of scope.
IR-5	Incident Monitoring	IR-5	Incident monitoring will be supported by advanced logging and auditing features of components, but agencies may wish to bolster these capabilities with additional monitoring tools.
IR-6	Incident Reporting	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and incident response is considered out of scope.
IR-7	Incident Response Assistance	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and incident response is considered out of scope.
Maintenance			
MA-1	System Maintenance Policy and Procedures	Not Selected	Agencies should already have policy and procedures for system maintenance. These will not be created for the purposes of this Model.
MA-2	Periodic Maintenance	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and maintenance activities are considered out of scope.
MA-3	Maintenance Tools	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and maintenance activities are considered out of scope.
MA-4	Remote Maintenance	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and maintenance activities are considered out of scope.
MA-5	Maintenance Personnel	Not Selected	This control does not apply. This Model is only

CNTL NO.	Control Name	"Moderate" 800-53A Requirements	Model Proposed Implementation/ Control
			meant to demonstrate functional capability and maintenance activities are considered out of scope.
MA-6	Timely Maintenance	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and maintenance activities are considered out of scope.
Media Protection			
MP-1	Media Protection Policy and Procedures	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and developing policy and procedure is considered out of scope.
MP-2	Media Access	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and media protection is considered out of scope.
MP-3	Media Labeling	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and media protection is considered out of scope.
MP-4	Media Storage	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and media protection is considered out of scope.
MP-5	Media Transport	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and media protection is considered out of scope.
MP-6	Media Sanitization	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and media protection is considered out of scope.
MP-7	Media Destruction and Disposal	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and media protection is considered out of scope.
Physical and Environmental Protection			
PE-1	Physical and Environmental Protection Policy and Procedures	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and developing policy and procedure is considered out of scope.
PE-2	Physical Access Authorizations	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and physical and environmental protection is considered out of scope.
PE-3	Physical Access Control	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and physical and environmental protection is considered out of scope.
PE-4	Access Control for Transmission Medium	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and physical and environmental protection is considered out of scope.
PE-5	Access Control for Display Medium	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and physical and environmental protection is considered out of scope.
PE-6	Monitoring Physical Access	Not Selected	This control does not apply. This Model is only

CNTL NO.	Control Name	"Moderate" 800-53A Requirements	Model Proposed Implementation/ Control
			meant to demonstrate functional capability and physical and environmental protection is considered out of scope.
PE-7	Visitor Control	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and physical and environmental protection is considered out of scope.
PE-8	Access Logs	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and physical and environmental protection is considered out of scope.
PE-9	Power Equipment and Power Cabling	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and physical and environmental protection is considered out of scope.
PE-10	Emergency Shutoff	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and physical and environmental protection is considered out of scope.
PE-11	Emergency Power	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and physical and environmental protection is considered out of scope.
PE-12	Emergency Lighting	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and physical and environmental protection is considered out of scope.
PE-13	Fire Protection	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and physical and environmental protection is considered out of scope.
PE-14	Temperature and Humidity Controls	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and physical and environmental protection is considered out of scope.
PE-15	Water Damage Protection	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and physical and environmental protection is considered out of scope.
PE-16	Delivery and Removal	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and physical and environmental protection is considered out of scope.
PE-17	Alternate Work Site	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and physical and environmental protection is considered out of scope.
Planning			
PL-1	Security Planning Policy and Procedures	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and developing policy and procedure is considered out of scope.
PL-2	System Security Plan	Not Selected	This control does not apply. This Model is only

CNTL NO.	Control Name	"Moderate" 800-53A Requirements	Model Proposed Implementation/ Control
			meant to demonstrate functional capability and developing and updating a system security plan is considered out of scope.
PL-3	System Security Plan Update	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and developing and updating a system security plan is considered out of scope.
PL-4	Rules of Behavior	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and developing rules of behavior is considered out of scope.
PL-5	Privacy Impact Assessment	PL-5	A privacy impact assessment will be preformed on this model, to demonstrate how a similar production system would be classified.
Personnel Security			
PS-1	Personnel Security Policy and Procedures	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and developing policy and procedure is considered out of scope.
PS-2	Position Categorization	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and personnel security is considered out of scope.
PS-3	Personnel Screening	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and personnel security is considered out of scope.
PS-4	Personnel Termination	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and personnel security is considered out of scope.
PS-5	Personnel Transfer	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and personnel security is considered out of scope.
PS-6	Access Agreements	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and personnel security is considered out of scope.
PS-7	Third-Party Personnel Security	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and personnel security is considered out of scope.
PS-8	Personnel Sanctions	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and personnel security is considered out of scope.
Risk Assessment			
RA-1	Risk Assessment Policy and Procedures	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and developing policy and procedure is considered out of scope.
RA-2	Security Categorization	RA-2	A risk assessment was preformed on this Model and it was categorized according to FIPS 199 to demonstrate how a similar production system would be categorized.
RA-3	Risk Assessment	RA-3	A risk assessment was preformed on this Model according to NIST 800-30, to demonstrate how a similar production system would fare.

CNTL NO.	Control Name	"Moderate" 800-53A Requirements	Model Proposed Implementation/ Control
RA-4	Risk Assessment Update	Not Selected	No updates will be made to the original risk assessment. This control is considered out of scope.
RA-5	Vulnerability Scanning	RA-5	Vulnerability scanning will be carried out on the Model using a Commercial off-the-Shelf (COTS) vulnerability assessment tool.
System and Services Acquisition			
SA-1	System and Services Acquisition Policy and Procedures	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and developing policy and procedure is considered out of scope.
SA-2	Allocation of Resources	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and allocation of resources are considered out of scope.
SA-3	Life Cycle Support	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and lifecycle support activities are considered out of scope.
SA-4	Acquisitions	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and system and service acquisition is considered out of scope.
SA-5	Information System Documentation	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and system documentation is considered out of scope.
SA-6	Software Usage Restrictions	SA-6	Endpoint enforcement components can evaluate the user's system for malicious software
SA-7	User Installed Software	SA-7	The user populations this Model targets will own the computers used to access the application. They will have administrative control over the system and the ability to install software of their choice.
SA-8	Security Design Principles	SA-8	This Model will be designed a built following best practices and guidance provided by NIST SP 800-27.
SA-9	Outsourced Information System Services	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and none of the services will be external or outsourced.
SA-10	Developer Configuration Management	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and configuration management is considered out of scope.
SA-11	Developer Security Testing	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and developer security testing is considered out of scope.
System and Communications Protection			
SC-1	System and Communications Protection Policy and	SC-1	This control does not apply. This Model is only meant to demonstrate functional capability and

CNTL NO.	Control Name	"Moderate" 800-53A Requirements	Model Proposed Implementation/ Control
	Procedures		developing policy and procedure is considered out of scope.
SC-2	Application Partitioning	SC-2	Application presentation and business services will separate user functionality both logically and physically.
SC-3	Security Function Isolation	Not selected	This control does not apply. This Model is only meant to demonstrate functional capability and it has been deemed unnecessary to isolate security functions for the purposes of this test.
SC-4	Information Remnants	SC-4	Components of this Model with prevent unauthorized and unintended information transfer via shared system resources.
SC-5	Denial of Service Protection	SC-5	Boundary protection devices will limit the potential for denial of service attack from affecting the Model.
SC-6	Resource Priority	Not selected	This control does not apply. This Model is only meant to demonstrate functional capability and resource priority control is considered out of scope.
SC-7	Boundary Protection	SC-7 (1)	Boundary protection devices (firewall) and endpoint enforcement components will be utilized to protect the Model at the system boundary.
SC-8	Transmission Integrity	SC-8 (1)	Integrity will be guaranteed by cryptographic mechanisms which will recognize any changes to information during transmission.
SC-9	Transmission Confidentiality	SC-9 (1)	Confidentiality will be guaranteed by cryptographic mechanisms which will prevent the unauthorized disclosure of information.
SC-10	Network Disconnect	SC-10	Application services will terminate network connections with a user at the end of a session.
SC-11	Trusted Path	SC-11	Cryptographic mechanisms will be used to create a trusted path will be created between the Model's application services and users.
SC-12	Cryptographic Key Establishment and Management	SC-12	Cryptographic keys will be managed by components of the Model, as prescribed by NIST SP 800-56 and 800-57.
SC-13	Use of Validated Cryptography	SC-13	All cryptography used in the Model will be FIPS 140-2 compliant.
SC-14	Public Access Protections	SC-14	Integrity and availability of publicly available information presented by Model applications will be protected.
SC-15	Collaborative Computing	SC-15	No collaborative components will be activated by any component of the Model.
SC-16	Transmission of Security Parameters	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and labeling is considered out of scope.
SC-17	Public Key Infrastructure Certificates	Not Selected.	This control does not apply. This Model is only meant to demonstrate functional capability and it will not be cross-certified with the Federal Bridge.
SC-18	Mobile Code	SC-18	Mobile code will be used by the endpoint

CNTL NO.	Control Name	"Moderate" 800-53A Requirements	Model Proposed Implementation/ Control
			enforcement component. Guidance on controlling this code from NIST SP 800-28 will be considered.
SC-19	Voice Over Internet Protocol	Not Selected	This control does not apply. Voice over IP will not be utilized for this Model.
System and Information Integrity			
SI-1	System and Information Integrity Policy and Procedures	SI-1	This control does not apply. This Model is only meant to demonstrate functional capability and developing policy and procedure is considered out of scope.
SI-2	Flaw Remediation	SI-2	All patches, service packs, and hot fixes will be installed on components of this Model.
SI-3	Malicious Code Protection	SI-3 (1)	The endpoint enforcement component will detect malicious code on user's system. Other malicious code protection tools, such as anti-virus software, will be used on mole components.
SI-4	Intrusion Detection Tools and Techniques	SI-4	Some components of the Model will have intrusion detection capabilities. However, production systems would want to implement additional intrusion detection tools and techniques.
SI-5	Security Alerts and Advisories	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and receiving security alerts and advisories is considered out of scope.
SI-6	Security Functionality Verification	SI-6	The functionality of all security components of the Model will be verified as working.
SI-7	Software and Information Integrity	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and routinely verifying software integrity is considered out of scope.
SI-8	Spam and Spyware Protection	SI-8	Endpoint enforcement components will attempt to detect spyware applications running on users' systems.
SI-9	Information Input Restrictions	Not selected	This control does not apply. This Model is only meant to demonstrate functional capability and adding additional information input restrictions to Model components is considered out of scope.
SI-10	Information Input Accuracy, Completeness, and Validity	SI-10	Application services will check information for accuracy, completeness, validity, and authenticity.
SI-11	Error Handling	SI-11	Some degree of error handling will be build into Model application services.
SI-12	Information Output Handling and Retention	Not Selected	This control does not apply. This Model is only meant to demonstrate functional capability and retaining system output is considered out of scope.

8.4 Summary of Risk Assessment Results for Model

Risk Assessment results for the Model design revealed several potential areas of concern as priority areas for further focus. The key concept centers on public trust and acceptance of the Secure Channel and the resulting channel usage. While these areas are not traditionally seen as "security" problems for government-controlled data within the scope of control of the traditional system, "secondary" security issues are emerging as a new problem. MITRE defined these "secondary" issues as security-related problems encountered outside the traditional government systems' hardware and software security boundaries.

These new generation risks specifically impact the public's trust and security perceptions of the core Citizen Channel Systems. In the past, the security of a Citizen's personal PC itself, vulnerability to data loss, vulnerability to password and ID compromise, and other Citizen/User responsibilities would be the primary responsibility of the Citizen with the resulting data or information loss limited to that Citizen and the Citizen's personal liability. However, with the increasingly complex and interconnected internet and the modern computing environment, a realization has come that there is now an extreme interconnectivity between all these Citizens systems. This interconnectivity creates a much higher potential for widespread data and information loss, or the perception of the same, across significant numbers of Citizens. It has created an emerging new dynamic in the security threat environment. In this new environment of Citizen to government processing, the vulnerability of the Citizen's unsecured personal environment and systems must be recognized and dealt with. In addition, this perception and impact of a perceived security threat must be recognized.

In this new paradigm, federal agencies are beginning to see how the loss of small amounts of data over a relatively small number of Citizens can cascade into a wave of Citizen distrust of government systems and a resulting backlash of a lack of utilization of the impacted government portal systems. The perception of insecurity can be as damaging as an actual large-scale data loss to the utilizations and therefore, the effectiveness of many of these potential Citizen Channel systems.

All these threats were reviewed and some additional focus was identified in the risk assessment of this Model. Two areas clearly emerged within the scope of this research Model where new technologies and methods were needed for mitigation. Areas for further investigation included:

- Security of Citizen host systems outside of the government-controlled firewall and security parameter.
- Two (2) Factor Authentication schemes and implementations technologies to support large-scale user populations realistically at appropriately-balanced levels of security vs. costs.

Controls and approaches to these areas of concern were added to the Model design and a second pass at the assessment was made. The Risk Mitigation planning then focused on planning for innovative solutions to these specific areas of risk.

8.5 Risk Mitigation Planning Summary

MITRE made an assumption that many traditional solutions outlined in the Risk Assessment Matrix (above) were relatively mature and available. These "standard" security controls and

tools are outlined in the previous security controls mapping. The focus for MITRE's activities was then shifted to identifying available new technology areas to investigate potential solutions for specific risk areas of interest for this Citizen Channel environment, as well as identify high likelihood problems associated with Non-Secure Citizen systems and effective and realistic authentication methods.

In order to effectively deal with a selected set of high-probability risks and threats that emerged from the risk analysis and assessment process, several specific products were focused on and investigated in the pilot demonstration. These products formed the key components of the pilot demonstrations and test. They were selected as representative products to contribute potential controls for discovered non-traditional, high-risk areas.

8.5.1 Key Risks Identified for Further Focus

The following key risks were identified for further focus:

- The security of the Citizen's computer is unknown and therefore MITRE assumes it has been compromised.
- Data transmitted over the channel could be read by an attacker while it is in transit
- If the government system is incorrectly programmed, it is probable that one Citizen may inadvertently see another Citizen's data.
- A Citizen may intend to supply personal information to the government, but may instead provide it to a rogue or fake site due to a social engineering attack, such as phishing.
- Large numbers of Citizens accessing a system at one time may put unrealistic loads and systems requirements on the government host systems.

8.5.2 Key Risk Mitigation Actions Implemented

The Secure Citizen Interaction Technology demonstrations showcase ways an endpoint enforcement system will react when faced with changes of the endpoint system state. These system states, combined with the variation in platform, will help to illustrate the current state-of-the-art in network admission technology. In addition, the work utilizes innovative alternative multi-factor authentication mechanisms.

This integrated process would involve full disclosure to the Citizen of the choice for an automated agent software element running on the Citizen's host computer to validate a minimal security policy configuration. Tools and processes would be utilized to investigate the configuration and security profile of the Citizens host computer actively. For the research demonstration a runtime Linux environment that will run Insightix (a post network admission control suite that monitors traffic and authorizes connectivity based upon users' platform security posture and role-based policy) to monitor the security policy and interactions.

The Citizen would be allowed to choose whether to allow this agent to execute on host system or to opt out and selects not to participate in the automated Secure Citizen Channel portal. If a Citizen elects not to participate, then information on alternative communications channels and methods would be provided.

The agent would confirm a minimal security policy on the host and allow access or the agent would indicate a suspected problem and refer the Citizen to other providers for corrective action

and not grant the citizen access. All agent processes would be contingent on a full-user authentication cycle before the agent processing would proceed.

Full-link encryption of all data in transit would be utilized to provide a level of security corresponding to the identified data security categorization and risk. The endpoint Citizen systems must have a reasonable level of security and assurance to utilize these standard link encryption products effectively. If the base Citizen platform is not secure, securing data in and out of that platform will be of limited value.

Full security risk and design reviews of the operational systems would be conducted to identify any risk of data sharing. Extensive test cases and testing is required to validate and certify an operational federal data system commiserate with the Security Categorization of the data elements and the processing sensitivity. However, specific details of the final operational application and system are beyond the scope of this research.

Although design solutions exist for an operational implementation, it is beyond the scope of this research. For example, this Model is only meant to demonstrate functional capability. It will not be cross-certified with the Federal Bridge.

Applications security, applications "isolation," and remote "Thin Client" applications were all considered and investigated as risk mitigation possibilities. Secure Virtual Private Network (VPN)-based remotely hosted thin client applications and systems are available. These technologies allow a user to run a specific custom, secure application on a Citizen PC and interact via a secure VPN connection with a remote host environment. All actual applications' processing is performed on the remote host machine. The Citizens PC becomes simply a "dumb terminal" running the keyboard and window application outside the normal Windows Browser environment. The concept depends on the assumptions that the new display and keyboard interface module and associated VPN are secure and that it provides an isolated secure application suite in an unsecured host PC "terminal" environment. This work has been focused in the remote agent direction due to the following two primary concerns:

1. A large amounts of the host server's processing power is required for a large-scaled environment that currently serves numerous concurrent users with this technology.
2. The security of the Citizen PC application and resistance to malicious code and agents are unknown and require additional specific research.

MITRE's approach is to improve Citizen Host PC Security. While this remote virtual session technology holds promise, due to performance and unknown Citizen Host PC security concerns and implications, it was determined by the MITRE Team to be outside its scope of this current research, key solution concepts, and available resources.

9. Phase 5—Model Technology Demonstration

Phase 5 is a strawman technology architecture and a demonstration of key concepts identified for further investigation. This technology demonstration will be a simple proof of concepts and demonstration of the candidate technologies that contribute key strengths to baseline Model security requirements.

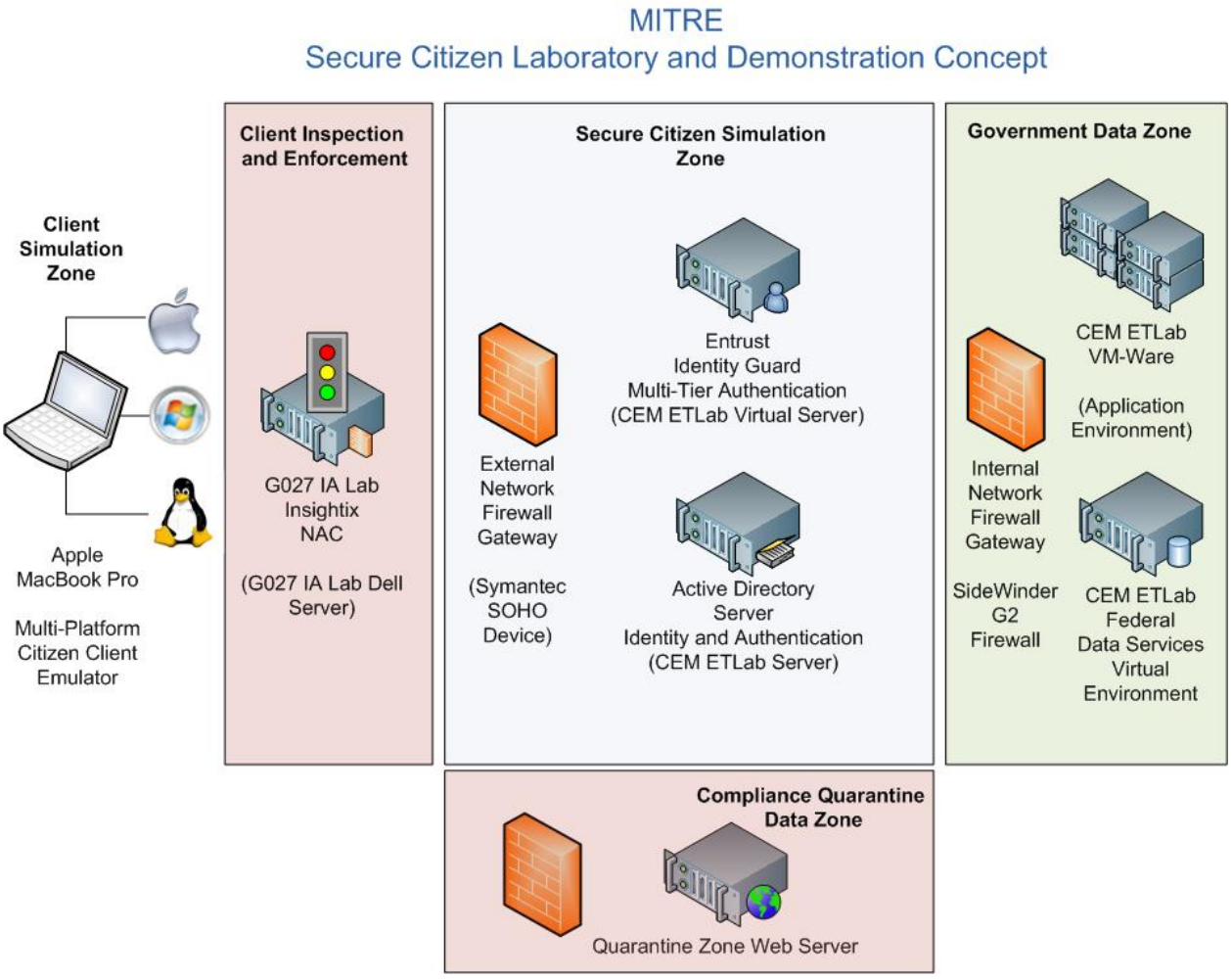

Figure 4. MITRE Secure Citizen Lab Concept

9.1 Laboratory Assets and Functional Mapping

The following section a describes lab assets and illustrates their functional position within the Secure Citizen Proof of Concept key technologies prototype system as illustrated in Figure 4.

Apple MacBook Pro

This workstation will act as the "public" platform, which will simulate all three major "Citizen possible" operating system environments (i.e., MAC, PC, and LINUX) on the same desktop using the new VMWARE Fusion product for the Mac.

Stand Alone Intel Server

This server provides the Endpoint Enforcement Device/Edge Protection Device. A runtime Linux environment that runs Insightix, a post network admission control suite that monitors traffic and authorize connectivity based upon users platform security posture and role-based policy.

Four (4) Virtual Windows 2003 Servers

These servers constitute the multi-tier application environment consisting of the following functional assets:

- Presentation Services—Internet Information Server used in presenting Web pages to the Citizen community of interest.
- Application Services—Web application server (e.g., .NET or Java-based service) that delivers business components to the Citizen application.
- Identity Service—Active Directory server that will carry user information at the edge to authenticate and provide access to application components through the Endpoint Enforcement Device.
- Business Services—calculation or collaborative service, such as MS SharePoint or other real-time collaboration and electronic messaging.
- Database (Store) Services—virtual server that will consist of an MS-SQL server instance, which will simulate the data tier of the multi-tier environment where data is stored and delivered in concert with access policies.

9.2 Secure Citizen Laboratory Demonstration Application and Technologies

9.2.1 Network Perimeter Control

Firewalls comprise the primary perimeter control and network separation duties within the Secure Citizen laboratory environment. At the edge, the network separation from the external network, as well as the routing to the network admission control environment, is done via a Symantec SOHO device. This device can perform rudimentary checks on port and protocol, as well as some simple authentication services.

9.2.2 Identity Management and Authentication

The identity management system for the Secure Citizen environment was based on the Entrust Identity Guard system. This system can consume identity data from a variety of identity data repositories and use this information in combination with multiple forms of second factor authentication services, such as smart tokens, smart cards, grid cards, and even knowledge-based authentication.

Passwords are the most commonly used form of single-factor authentication. Two-factor authentication requires more then just "what you know." Using additional factors can help increase confidence in the identity of the user. Currently, hardware one-time password (OTP) tokens are the most common form (i.e., SecurID). The compromise of any one of the two factors does not yield access.

MITRE's focus for this area of the technical dimension was on how sponsors could meet two-factor authentication requirements when dealing with the following:

- Very large, variable user populations
  - Could include support for population sizes in the millions
  - Numbers of concurrent users may fluctuate greatly based on a variety of factors, some of which may be unpredictable
  - Users will not be limited to government employees and contractors
- Populations of users that require different levels of protection
  - There may be many different classes of users for the same system, all of which require access to information of varying sensitivity
- Diverse computing platforms that the agencies cannot control
  - Sponsors will have very little, if any, control over a user's hardware and software

These constraints present challenges when looking to use common two-factor authentication technology, like hardware OTP tokens and PKI-based solutions. For example, OMB 06-16, requires two-factor authentication any time Personally Identifiable Information (PII) is present.

> "Allow remote access only with two-factor authentication, where one of the factors is provided by a device separate from the computer gaining access."

After talking with different government organizations, MITRE recorded the following observations:

- Government organizations often need additional guidance on how to implement two-factor authentication:
  - Difficult to support and deliver hardware tokens to highly-variable or Citizen populations
  - Cost of hardware tokens is prohibitive for organizations with a very large user base
- Some regulations are confusing and do not address all options:
  - OMB 06-16 partially contradicts the guidance in NIST 800-63
  - NIST 800-63 does not address technologies that are becoming common in the financial service market, such as knowledge-based authentication and grid cards
- New technology is rapidly being introduced to the market:

- It is often difficult to separate what the technology offers from the marketing
- Many approaches are still maturing—there are few market leaders

A high-level market survey revealed that vendors' solutions that were reviewed primarily make use of the following authentication mechanisms:

- OTP Token-Based Authentication
- Knowledge-Based Authentication
- Message-Based Authentication
- Device-Based Authentication
- Grid Card/One Time Password

MITRE evaluated two products in the lab to gain a better understanding of these mechanisms:

- StrikeForce ProtectID and Entrust IdentityGuard—The final demo selection was based upon the variety of mechanisms supported and vendor cooperation/ availability.
- MITRE did not review biometric or smart card-based solutions, whose technologies were considered out of scope based on MITRE's stated focus.

In the end, non token-based methods were considered favorable due to costs and the logistics for this work.

9.2.3 User Repository

For the purpose of the laboratory environment, a Microsoft Active Directory server was provisioned with the necessary extensions to house both unique authentication attributes needed by Entrust, as well as group policy information to assist the Insightix network discovery and admission control system. The Active Directory was considered a "border directory" for the purpose of the laboratory setup. A directory of this type is used with customer-facing services and is separated from the internal assets of the organization. This directory did not contain PII thus it did not incur the same scrutiny as an internal directory would have.

9.2.4 Post Network Admission and Client Compliance

The keystone technology for the Secure Citizen demonstration and lab was the use of advanced network admission technology. This technology is designed to interrogate the security posture of an incoming (or outgoing) client on the network and decide access based on the level of policy compliance the client has achieved. This compliance can be a rich set of configuration parameters that may be discovered by a "dissolvable" agent, which can be downloaded onto the Citizen platform.

For the technology demonstration, this set of configurations parameters was set to a minimal default set as provided by the Insightix product. The purpose of the demonstration was to explore the core operations capability of the remote agent software to detect minimal fundamental incoming client configurations as a proof of concept.

The Insightix (Enterprise Version 4) product operates without directly impacting the network connection through a layer 2 discovery. Once the host is discovered, the network admission proxy looks at the client parameters through a passive discovery of the client and then allows for either Windows Management Instrumentation (WMI) direct interface through the Win32 API or

the install of a JAVA-based client for Macintosh and Linux platforms. When and if, the client passes the policy tests, the device allowed access to the network.

9.2.5 Technology Demonstration Walkthrough

Figure 5 illustrates a step-by-step process by which the demonstration laboratory environment explores and highlights possible solutions to the network admission and flexible authentication problems described in the above sections.

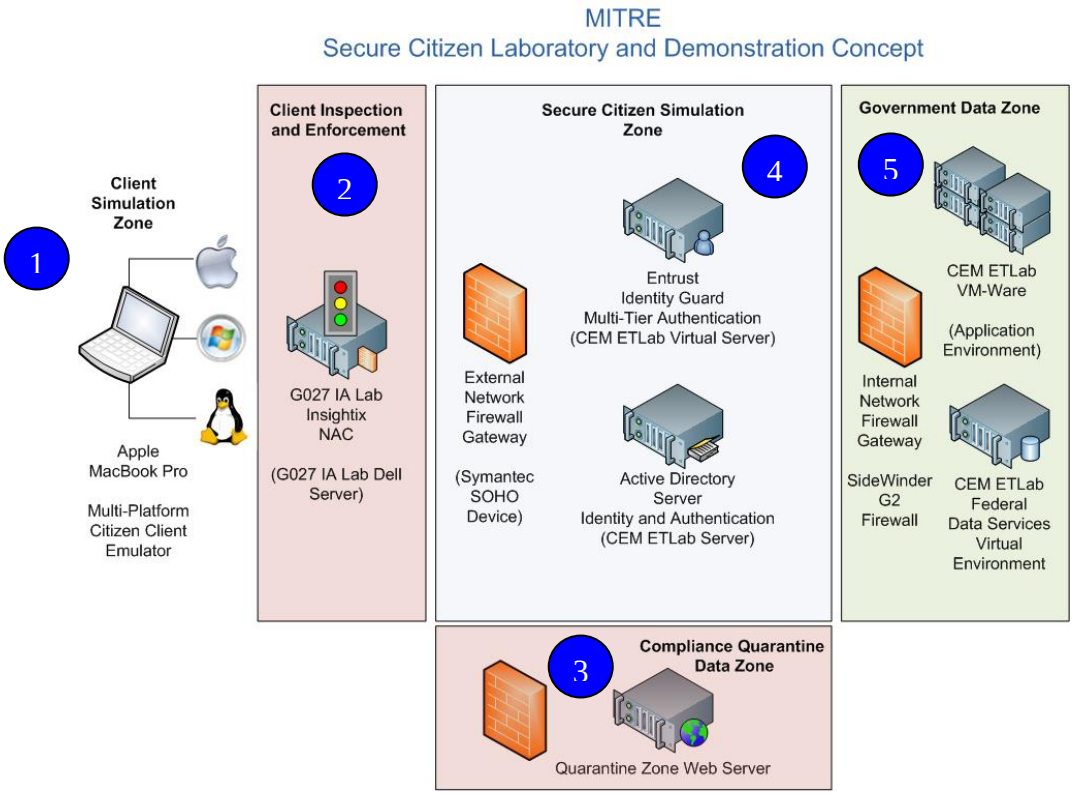

Figure 5. Mapping of Demonstration Steps

1

Step 1: User Initial Request for Service—user attempts to initiate a connection to the federal system portal application via a standard URL

2

Step 2: Consent for Admission Scan—service delivery point notifies the user that they must consent to their system being assessed by the endpoint device prior to admission to the federal system. The consent describes the scan criteria based upon declared platform (mac,pc,linux) and asks the user to allow access by the endpoint enforcement agent via a downloadable control.

Step 3: Redirect or Termination—if the user agrees to the scan then the system redirects the user to the endpoint enforcement device. If the user declines the scan then the system terminates the connection and describes the alternative methods for interaction.

Step 4: Scan Initialization—endpoint enforcement device delivers a dissolvable agent to the user platform and initiates the scan to determine the state of the endpoint.

Step 5: Scan Results and Reporting—user is notified of his/her state and scan results. The user is given a redirect to the next step of access based upon the state of their system:

- **Compliant—**user is directed to the user authentication portal and endpoint enforcement dissolves the agent on the user's system.
- **Deficient—**user is given a report on system deficiencies and links to remediation patches or a platform security site. The user is given the option of limited access to services and is sent to authentication to the limited service area.
- **Compromised—**user is given a warning that his/her system has been compromised. The user is given basic directions to limit further exposure and the user's connection is terminated.

Step 6: User Authentication Registration—user is given the opportunity to be provisioned into the system using an acceptable form of second factor device or questions for self-service registration.

- **Compliant User Registration—**user registers the device to the system
- **Deficient User Registration—**user is asked knowledge-based questions to form initial registration.

Step 7: User Authentication—user is asked to authenticate using accepted form of authentication technology. For this demonstration, a cell telephone was used as a independent, second factor, hardware token.

Step 8: User Access—compliant user is allowed full access to the system. The deficient user is allowed access to the restricted access area.

9.3 Observed Results of Technology Demonstration Runs

The Model's technology demonstrations and experimental proof of concept runs provided three significant key results and findings.

- **Finding 1:** Many creative and flexible commercially-available (COTS) authentication methodologies and technologies exist. These technologies can perform reasonable two-factor authentications without expensive and logistically challenged hardware tokens in most cases. Scalable solutions exist for Secure Citizen Interaction Channel implementations.
- **Finding 2:** COTS Network and Visibility technologies were demonstrated to confirm the security profile and required minimal security policies of a Citizens PC via the execution and reporting of a "remote agent" application kernel on the Citizen's computer. These technologies can be integrated into existing security portal environments and designs. They can be effectively tailored to return detailed information on critical computer application and operating system configurations and statuses per a preconfigured minimal security profile for the specific Secure Citizen Interaction Application.
- **Finding 3:** These COTS Citizen computer agent technologies can be configured to only download and run with Citizens' permission, not to retain this data, to report back to the Citizen suggestions for required improvements to the Citizens system if policy-based access is denied, as well as to also allow different levels of access to host government systems.
- **General Finding:** Overall, many of the major weaknesses and security risks can be contained with some creative and tailored COTS solutions for the specific government security requirements as outlined in the "Moderate" Model defined in this research. However, some of these solutions require a forward-looking anticipatory approach to security design versus the traditional security problem and reactive mode of design and operations.

10. Summary

For this research Model, MITRE followed the process steps (per NIST 800-30) previously listed. The summary results are:

System Characterization

The representative Civil "system" Model was constructed from similar real world federal data and systems' specification components. The Model's type and data mix was selected as a realistic and representative mix of systems. When this mixture of data types and systems' type requirements were put through the required evaluation and analysis, a moderate security confidentiality, impact and availability requirement was defined as a representative baseline for the data mix and systems' types reviewed.

Threat Identification

Threat analysis revealed that there were four major new threat areas specific to the Secure Citizen aspect of this Federal Civil System.

1. The security of the Citizen's computer is unknown; therefore, MITRE assumes it has been compromised.
2. Data transmitted over the channel could be read by an attacker while in transit.
3. If the government system is incorrectly programmed, it is probable that a Citizen may inadvertently see another Citizen's data.
4. A Citizen may intend to supply his personal information to the government, but may instead provide it to a rogue or fake site due to a social engineering attack, such as phishing.

Vulnerability Identification

The key vulnerabilities discovered in this research focus on those vulnerabilities created by a large pool of unsecured, uncontrolled Citizen PCs requiring access to secure government systems in a reasonably secure mode. Authentication and other traditional security vulnerabilities are also contributing factors to the overall vulnerability profile of this type application or channel system.

Control Analysis

The traditional 800-53 Control analysis has highlighted the need for new and innovative technologies to provide mitigating controls for identified new risks and vulnerabilities.

Likelihood Determination

The likelihood of the threats occurring is Moderate to High if the new generation of authentication and endpoint enforcement mitigation and controls are not implemented to augment the traditional security controls for this specific type of Secure Citizen Channel and environment.

Impact Analysis

The impact to the government and the Citizen could be Moderate from the included analysis of the data and system types included in this research.

Risk Determination

The data classification (in "Summary") for the research Model and its associated data remains at the **Moderate level**. All data was conservatively classified as Privacy Act Data, which will be the basis for the design and Security Risk Assessment.

Controls

The research focused on augmenting the traditional controls and processes as outlined on MITRE's Model based 800-53 analysis ***with strong multifactor user authentication and innovative endpoint enforcement systems.***

Results

The technology demonstrations, based on emerging, commercially-available technologies, offer a strong potential for effective risk mitigation as well as provide an efficient balance of security to costs and operational requirements for key concern areas for the new generation of Citizen Secure Internet Channels. More focus and effort should be made on these specific emerging technology areas for this type of application and Secure Citizen Channel.

11. Conclusions

In this document, MITRE has outlined a generalized framework to investigate a potential approach for a U. S. Agency's use of a Secure Channel to interact with Citizens. MITRE has shown that it is possible to integrate a set of existing processes to define and document an operationally secure, risk-balanced, and effective Citizens Interaction Channel. This set of technologies can include a method of assuring that a personal PC system used by Citizens will not compromise the channel's security.

This document also formulates the generalized approach that an agency could take to establish a Secure Channel over the internet for interacting with Citizens. Sample requirements were defined and a baseline technical architecture presented in addition to a potential demonstration solution.

MITRE presented a representative set of data similar to what could be collected from Citizens, as well as extended assumptions on how this set of information might be utilized. The sensitivity level associated with the representative information and system was ascertained as Moderate. A PIA of collecting and maintaining the information was presented.

This research looked into potential solutions and technologies to provide a usable Secure Citizen Channel. Based on the sensitivity of the collected data and the operational scenario, the demonstration system presents several approaches to Citizens' e-authentication that are appropriate for the required level of assurance. The Citizens' options for using the channel are also considered and realistic options presented.

The Model design has resulted in a generic system and specific technology demonstrating the integration of technologies in support of the developed framework.

This research has provided a structured approach to the required analysis and presented MITRE's findings by NIST required area. The final focus was on the significant risk areas of authentication and endpoint enforcement encountered. MITRE then identified, potential, new technology alternatives.

In summary, while there are still significant challenges not mitigated directly in this research, it is clear that there are emerging technologies that could significantly reduce the risk of implementing these Secure Citizen Channels. Overall, many of the major weaknesses and security risks can be contained with some creative and tailored COTS solutions for the specific government security requirements as outlined in the "Moderate" Model defined in this research. However, some solutions require a forward-looking anticipatory approach to security design versus the traditional security problem and reactive mode of design and operations. Helping the Citizen to better secure an inherently unsecured Citizen PC is one example.

There is also a set of existing federal component standards, guidelines, and orders available to define and specify the minimal requirements for fielding an effective and compliant Secure Citizen Channel Program. The current challenges of multiple, sometimes conflicting, agency-specific security guidance can be effectively overcome by a systematic application of available NIST, FISMA, FIPS, OMB, or other federal standards and guidance.

MITRE recommends that the government should conduct further research with a focus on the emerging technologies in support of specific Secure Citizen Interaction Channel risk mitigations as outlined initially in this research.

Acronyms

CBA	Cost Benefit Analysis
CEM	Center for Enterprise Modernization
CMS	Centers for Medicare & Medicaid Services
COTS	Commercial off-the-Shelf
DHS	Department of Homeland Security
DoB	Date of Birth
e-Gov	e-Government or Electronic Government
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IR&D	Internal Research and Development
IT	Information Technology
ITL	
LAN	Local Area Network
MITRE	The MITRE Corporation
NAC	Network Admission Control
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
OGA	other government agency
OMB	Office of Management and Budget
PC	personal computer
PIA	Privacy Impact Analysis
PKI	Public Key Infrastructure
PoB	Place of birth
SC	Security Category
SP	Special Publication
SSN	Social Security Number
TBD	To be Determined
VLAN	Virtual LAN
VPN	Virtual Private Network

OTP one-time password

URL