DIVS

Privacy and Security Program Framework

For Vendors, Developers and Suppliers

Version 1.6

December 21, 2015

This Document was prepared under a grant from the Federal Emergency Management Agency's (FEMA) Grant Programs Directorate (GPD) United States Department of Homeland Security. Points of view or opinions expressed in this document are those of the authors and do not necessarily represent the official position of policies of FEMA/GPD or the U.S. Department of Homeland Security.

This document and associated work product were produced by Clerus Solutions, LLC as Program Manager to the DL/ID Verification Systems, Inc. program under contract to the Mississippi Department of Public Safety.

TABLE OF CONTENTS

1 DIVS PRIVACY AND SECURITY PROGRAM FRAMEWORK

1.1 *DIVS Privacy and Security Program Framework Document Scope*

The DIVS Privacy and Security Program Framework (the 'Framework') document is intended for use by the DIVS Program Office to disseminate to all vendors, developers, or suppliers ('VDS') that will be participating in the Request For Proposal process. The expectation is that each VDS will utilize the Framework as a basis for its Privacy and Security program for all development, operation, support and use of the DIVS systems[1] including components managed by the VDS service providers on behalf of the VDS.

[1] With the sole exception of the users, these will be referred to collectively as 'Vendors, Developers or Suppliers' or 'VDS'.

1.2 *DIVS Privacy and Security Program Framework Status*

Table 1 Document Status

Item	Status
Document Title	DIVS Privacy and Security Program Framework for Vendors, Developers and Suppliers
Disposition/Status	**Approved**
Primary Contact, Organization	David Ezell, Mississippi Department of Public Safety
Secondary Contact, Organization	Luke McAlpin, Mississippi Department of Public Safety

1.3 *DIVS Privacy and Security Program Framework Revision History*

Table 2 Document Revision History

Version	Date	Author(s)	Description of Changes	Executive Committee Approval Date
Privacy and Security Plan Framework				
0.1	10/5/2009	Clerus Solutions	Initial Draft	
0.2	10/15/2009	Clerus Solutions	Accepted change on DIVS P&S committee classification decision and corrected formatting	
1.0	10/20/2009	Clerus Solutions	Approved version	10/20/2009
1.1	11/30/2010		In *Appendix A: Acronyms, Terms and Definitions,* replace definition of "Accreditation" with "Authorization". For reference to NIST SP 800-34, add "rev 1" and change "6/2002" to "5/2010". For references to NIST SP 800-37 (a) Remove "DRAFT" and replace "8/2008" with "2/2010"; (b) Update document title; (b) Update chapter and section titles chapters to titles as in SP 800-37. For reference to NIST SP 800-53A, add "rev 1" and change "7/2008" to "6/2010": update document title. For references to NIST SP 800-122, (a) Remove "DRAFT" and replace dates from "Jan 2009" with "April 2010" or from "1/2009" to "4/2010"; (b) Update title for Section 4.1.2 to match that in SP 800-122. For reference to NIST SP 800-128, replace "TBD" with "DRAFT"; add draft title.	2/15/2011

Version	Date	Author(s)	Description of Changes	Executive Committee Approval Date
Privacy and Security Plan Framework				
1.2	12/15/2011		Change frequency for all reviews and assessments from "periodic" to "annual" including: • Conducting ongoing risk and control assessment • DIVS Program Office's review of VDS compliance". For NIST SP 800-39, remove "DRAFT", update title and date. For reference to NIST SP 800-63 Rev 1, replace date with "6/2011", add "DRAFT" to title. For reference to NIST SP 800-128, remove "DRAFT"; replace date with "8/2011"; update title.	2/21/2012
1.3	4/29/2013	Clerus Solutions	Update all references of SP 800-53 to Revision 4 released on 4/30/2013. Update Appendix C with new and updated document reference information as well as move privacy controls to new Appendix D Add Appendix D documenting privacy controls as specified in new Appendix J in SP 800-53, Rev. 4.	4/29/2013
1.4	4/17/2014	Clerus Solutions	Update Appendix C and D with updated information for referenced documents. Minor formatting changes for uniformity with other DIVS documents.	4/17/2014
1.5	12/11/2014	Clerus Solutions	Update Appendix C and D with current information for referenced documents.	12/11/2014
1.6	12/10/2015	Clerus Solutions	Addition of footnote in Section 3 noting the amendment of FISMA 2002 by the Federal Security Modernization Act (FISMA) of 2014 Addition of FISMA of 2014 to Appendix A Update of Appendix C and D with current information for referenced documents	12/10/2015

1.4 *DIVS Program Privacy and Security Program Framework References*

1. Appendix A: Acronyms, Terms and Definitions

2. Appendix B: Summary of Framework Requirements
3. Appendix C: Framework Reference Documents – Security Controls
4. Appendix D: Framework Reference Documents – Privacy Controls
5. Attachments

    DIVS Privacy Policy for DIVS Vendors, Developers and Suppliers

    DIVS Security Policy for DIVS Vendors, Developers and Suppliers

2 INTRODUCTION

The privacy and security controls to protect the DIVS information systems and data are critical as the loss of data privacy / confidentiality, integrity or system availability can not only effect the operation of the DIVS systems but may bear negative regulatory, financial and reputational consequences. It is imperative that a well-planned privacy and security program is in place for all DIVS systems to reduce the risk of system compromise. This document provides a Framework for instituting a comprehensive privacy and security program. Although this is not a policy or requirements document per se there are specific requirements that must be met that either support the policy tenets in the DIVS Privacy Policy and DIVS Security Policy, or are general requirements for the VDS that will be managing DIVS systems. In either case, each requirement will be notated in this document and summarized in Appendix B.

Disclaimer: *This is a Framework for developing a Privacy and Security Program and provides guidance and references to the development of the program. Although it provides a Framework based on NIST, it is not intended to reference all applicable NIST publications.*

3 FRAMEWORK OVERVIEW

The Framework was developed to provide the VDS with a model and guidance for creating or extending an existing privacy and security program for the DIVS systems. This Framework is tailored after the National Institute of Standards and Technology (NIST) Special Publications (SP) documents that provide recommendations for privacy and security controls in order to protect the confidentiality, integrity, and availability of systems and their associated information assets. The NIST Special Publications were developed in support of the Federal Information Security Management Act of 2002 (FISMA)[2] which requires all Federal agencies to implement structured programs for information security.

Depending on the criticality of a system, NIST assigns a set of controls whereas a system categorized as ***high*** has the most stringent control requirements, ***moderate*** has a lesser stringent

[2] In December, 2014, the original FISMA of 2002 was amended by the Federal Information Security Modernization Act (FISMA) of 2014. Refer to www.dhs.gov.fisma for details of the new law.

control set and *low* the least stringent. There is a process for assigning the system category[3] and the determination was made by the DIVS Privacy and Security sub-committee to assign a *moderate* level for the DIVS systems. Additionally, NIST provides guidance on categorizing Personally Identifiable Information (PII) [4] and likewise a *moderate* level was assigned. All reference to the privacy and security controls are based on the *moderate* level of privacy and security controls.

The core components of the Framework are governance, the specific areas of privacy and security controls, ongoing risk and control assessment, continuous monitoring of the appropriate controls, and program improvement through remediation of control gaps. The intent is that the Framework will provide a roadmap for the required controls, remediation of gaps, and the continuous improvement of privacy and security protections as part of an ongoing program. Figure 1 provides an illustration of the Framework.

Although the Framework is based on NIST, the majority of controls and process requirements are similar to other established security models including ISO/IEC 27001.[5] Existing VDS privacy and security programs that are based on models such as ISO/IEC 27001 can be readily leveraged and mapped to the NIST Framework controls and processes.

REQUIREMENT 1: *Each VDS must develop a plan to either implement a privacy and security program OR augment an existing program, to address the intent of the NIST privacy and security controls specified in the Framework. This must be completed and disseminated to the DIVS Program Office within twelve months of contract agreement.*

[3] See Federal Information Processing Standards (FIPS) Publication 199 (Feb 2004) *Standards for Security Categorization of Federal Information and Information Systems* and NIST SP 800-60 (Aug 2008) *Volumes 1 and 2: Guide for Mapping Types of Information and Information Systems to Security Categories*
[4] See NIST SP 800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (April 2010)
[5] See NIST SP 800-53 Revision 4 (April, 2013) Appendix H that provides security control mappings to ISO/IEC 27001

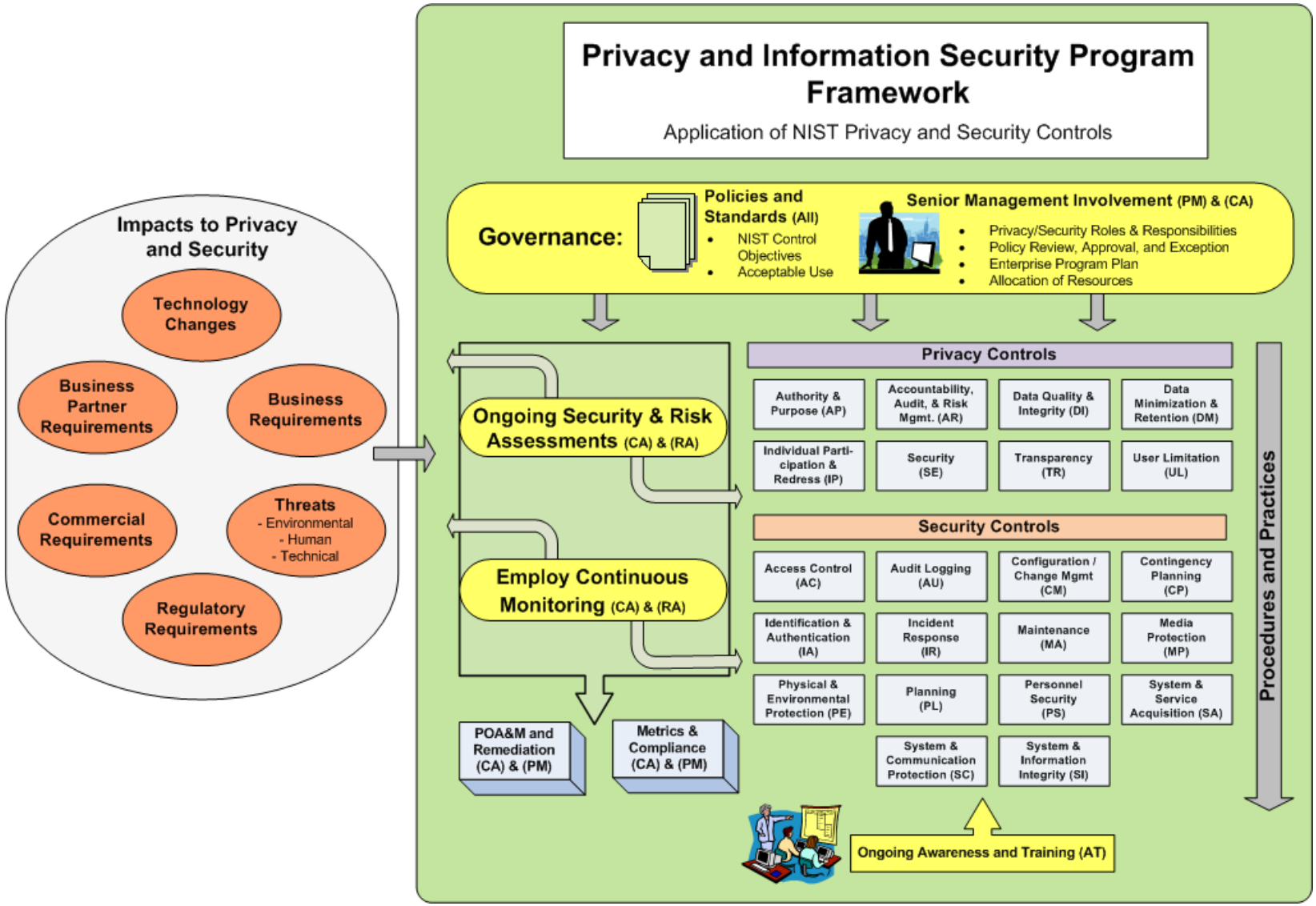
Privacy and Information Security Program Framework
Application of NIST Privacy and Security Controls
Impacts to Privacy and Security
Technology Changes
Business Partner Requirements
Business Requirements
Commercial Requirements
Threats
- Environmental
- Human
- Technical
Regulatory Requirements
Governance:
Policies and Standards (All)
NIST Control Objectives
Acceptable Use
Senior Management Involvement (PM) & (CA)
Privacy/Security Roles & Responsibilities
Policy Review, Approval, and Exception
Enterprise Program Plan
Allocation of Resources
Ongoing Security & Risk Assessments (CA) & (RA)
Employ Continuous Monitoring (CA) & (RA)
POA&M and Remediation (CA) & (PM)
Metrics & Compliance (CA) & (PM)
Privacy Controls
Authority & Purpose (AP)
Accountability, Audit, & Risk Mgmt. (AR)
Data Quality & Integrity (DI)
Data Minimization & Retention (DM)
Individual Participation & Redress (IP)
Security (SE)
Transparency (TR)
User Limitation (UL)
Security Controls
Access Control (AC)
Audit Logging (AU)
Configuration / Change Mgmt (CM)
Contingency Planning (CP)
Identification & Authentication (IA)
Incident Response (IR)
Maintenance (MA)
Media Protection (MP)
Physical & Environmental Protection (PE)
Planning (PL)
Personnel Security (PS)
System & Service Acquisition (SA)
System & Communication Protection (SC)
System & Information Integrity (SI)
Procedures and Practices
Ongoing Awareness and Training (AT)

Figure 1

4 THE FRAMEWORK COMPONENTS

4.1 *General Framework*

The purpose of the Framework diagram in Figure 1 is to provide a simple yet inclusive representation of the core elements of NIST. The Framework addresses all NIST security and privacy control 'families' outlined in NIST SP 800-53 Revision 4.

The security control identifiers notated in parenthesis in Figure 1 are as follows:

(AC) Access Control

(AT) Awareness and Training

(AU) Audit and Accountability

(CA) Security Assessment and Authorization

(CM) Configuration Management

(CP) Contingency Planning

(IA) Identification and Authentication

(IR) Incident Response

(MA) Maintenance

(MP) Media Protection

(PE) Physical and Environmental Protection

(PL) Planning

(PS) Personnel Security

(RA) Risk Assessment

(SA) System and Services Acquisition

(SC) System and Communications Protection

(SI) System and Information Integrity

(PM) Program Management

While most of the security controls families cover a specific area, a few, such as Program Management (PM), apply to several components in the Framework.

NIST provides a "Privacy Control Catalog" in Appendix J of SP 800-53, Revision 4, which documents privacy controls, enhancements, and supplemental guidance. These privacy controls include:

AP – Authority and Purpose

AR – Accountability, Audit, and Risk Management

DI – Data Quality and Integrity

DM – Data Minimization and Retention

IP – Individual Participation and Redress

SE – Security

TR – Transparency

UL – Use Limitation

Appendix C and Appendix D in this Framework provide references and descriptions to the NIST Special Publications and other pertinent references and guides to assist the VDS to institute a privacy and security program to align with the Framework.

4.2 *Impacts to Privacy and Security*

The incentive for implementing and maintaining a privacy and security program is primarily driven by a number of impact areas that could either disrupt the operational functions or negatively affect the reputation or financial well-being of an organization due to non-compliance. Additionally, an organization may be legally accountable to protect Personally Identifiable Information (PII) or effectively manage systems that could affect public safety. Below are the types of impacts that the VDS should take into consideration when conducting ongoing risk and security controls assessments (see Section 4.6) and employing continuous monitoring (see Section 4.7) as these are areas that could impact an existing privacy and security program:

- Technology Changes that can impair existing controls or introduce new vulnerabilities.
- Business Requirements that change the landscape (e.g., new business functionality in a system requires modification of access rights and increased levels of availability / recovery objectives).
- Threats including the following:
    - *Environmental* threats (e.g., storms, fire, pandemics, etc.) that can lead to power disruptions or personnel unavailability.
    - *Human* threats that can involve either internal or external personnel and be either intentional (e.g., hacking, theft, espionage) or unintentional (e.g., procedural errors, unintended data leakage).
    - *Technical* sources of threats which include hardware and software failures.
- Regulatory Requirements include compliance to Federal or State regulations (e.g., Drivers Privacy Protection Act). Changes in regulatory requirements can impact existing privacy or security program initiatives and the level of compliance that may currently be in place.
- Commercial Requirements include areas such as the Payment Card Industry (PCI) data security standards that can have applicability to system operations or modify the level of existing privacy or security controls.
- Business Partner Requirements include privacy and security expectations set forth by parties that are requesting managed provider services, system development services or other services. The expectations may be included in Request for Proposals and subsequently in contractual agreements.

4.3 *Governance*

Generally speaking, governance involves *defining expectations* and *providing oversight* for the policies, procedures, and practices used to fulfill those expectations. Governance is an essential component for the privacy and security program and is the foundation for the program.

4.3.1 *Policies and Standards*

The first priority for the privacy and security program should be the establishment of privacy and security policies. As indicated in Figure 1, policies are applicable to all NIST control areas so if the policies already exist in the VDS organization or if new policies are to be developed, they must address the controls applicable to a ***moderate*** level information system, including the development of Rules of Behavior ('Acceptable Use Policy'). The DIVS Privacy Policy and DIVS Security Policy can be utilized as foundational documents for the development of policies or updates to existing polices.

REQUIREMENT 2: *Each VDS must develop policies that address all NIST control objectives applicable to a* ***moderate*** *level information system and include Rules of Behavior ('Acceptable Use Policy').*

It is at the discretion of the VDS as how to format the policies (i.e., one large policy manual vs. several smaller policies which contain similar control families such as Access Control and Identification / Authentication). It is recommended that the 'Acceptable Use Policy' is a separate document given the target audience is general users. As a good practice, a defined process for policy development and deployment is recommended which includes these five steps:

1. Create a Policy Drafting Body to assign responsibility for drafting and reviewing policies. This may include scheduling workshops and review sessions during the course of policy development.
2. Define the Control Objectives - it is strongly recommended that NIST SP 800-53 Rev. 4 and NIST SP 800-122 are utilized.
3. Assign Policy Approval responsibilities as part of the privacy and security steering committee charter.
4. Communicate policy utilizing the awareness and training plan.
5. Develop a Policy Exception procedure.

REQUIREMENT 3: *Policy exceptions must be formally documented and approved. Any policy exceptions that may have significant bearing on the privacy / confidentiality, integrity, or availability of the DIVS systems or information must be reviewed and approved by the DIVS Program Office.*

4.3.2 *Senior Management Involvement*

Oversight of the privacy and security program should involve senior management including the establishment of a steering committee representing each of the core business areas and defining a charter that spells out its mission, responsibilities, membership, and authority. The steering committee must also ensure that specific organizational roles and responsibilities are defined and documented including assignment of an Information System Security Officer (or the equivalent), privacy officer(s), and continuity of operations emergency coordinator. The privacy and security responsibilities for other key stakeholders (e.g., System Owners, Human Resources personnel, Information Technology personnel) should be defined as well.

Another key deliverable for the steering committee is a privacy and security program plan, which is updated at least annually, that provides a summary of control status as well as plans for remediating control gaps, addresses organizational changes and issues, and identifies key metrics to measure program effectiveness.

REQUIREMENT 4: *A senior management oversight committee is to be established to define organizational privacy and security roles and responsibilities, approve policy and policy exceptions, develop a privacy and security program plan, and ensure that the appropriate privacy and security personnel are assigned for the program.*

4.4 *Privacy and Security Controls: Procedures and Practices*

The implementation of polices and standards themselves are controls but their purpose is to define the high level privacy and security control objectives and articulate 'what' must be fulfilled (e.g., change management must be instituted for all system configuration updates). The next level down further defines the control objective details and describes 'how' the objectives will be fulfilled. This involves a more tactical approach and the development of procedures and practices to incorporate the control objectives defined in policy. Appendix C and Appendix D provide recommendations for reference material to develop procedures or practices.

REQUIREMENT 5: *The VDS must develop procedures or practices to facilitate the implementation of the policy objectives for privacy and each security control family.*

4.5 *Awareness and Training*

Ongoing Awareness and Training is an integral component of the Privacy and Security Program and is pervasive to almost all areas of the controls. A core component of this control is the Awareness and Training Plan which defines specific responsibilities for awareness and training, tracking of training records, and guidance for conducting a 'needs assessment' to ascertain what areas should be targeted for awareness or training.

Given the presence of Personally Identifiable Information (PII) in the DIVS systems, priority should be given to PII protection as a topic for an initial awareness session.

REQUIREMENT 6: *The VDS must develop an Awareness and Training plan to address the control objectives defined in policy. Initial focus on awareness and training should be on privacy and the protection of PII.*

4.6 *Ongoing Risk and Control Assessments*

The management of risk is an essential component of the privacy and security program and should be the basis for decisions concerning priority of control implementation or gap closure. The risk assessment is an ongoing process and evaluation of changes to the impacts to Privacy and Security is essential to determining changes in the program, including any changes that may impact the categorization of the system. A formal assessment of the controls should also be conducted annually to identify gaps (in concert with the risk assessment) and evaluate the

effectiveness of the controls. A formal assessment of controls should also be conducted when any significant system updates are made.

REQUIREMENT 7: *The VDS must incorporate, as part of the privacy and security program, an ongoing process for risk assessment and control assessment. The VDS must conduct initial risk and privacy impact assessments for all DIVS systems for which they have been assigned as owners prior to acceptance in production.*[6]

4.7 *Employ Continuous Monitoring*

A common pitfall in addressing privacy and security is that it is treated as a one-time project to meet a point in time compliance requirement. The issue is not 'compliance vs. privacy/security' – compliance contributes to a secure environment – but *maintaining* the compliance.

Two primary factors contribute to drifting from compliance: (1) changes in the impact areas and (2) deviation from procedures or practices that support the control objectives. In order to facilitate *ongoing* compliance, key controls are to be continuously monitored for deviations.

REQUIREMENT 8: *The VDS must develop a strategy to ensure that key control areas are continuously monitored for deviation. Various tools can be utilized including configuration management software that identifies and alerts for unplanned changes, data integrity tools, intrusion prevention/detection technologies, and vulnerability scans.*

4.8 *Plan of Action and Milestones for Remediation*

To address existing control gaps and when control updates are needed to address weaknesses uncovered through the risk assessment, control assessment, or continuous monitoring, a documented Plan of Action and Milestones (POA&M) is to be developed. The POA&M must identify the weakness and lay out a plan for remediation.

REQUIREMENT 9: *The VDS must develop a formal POA&M template to document, in a consistent manner, the tracking of weaknesses ('control gaps') and plans for corrective action.*

4.9 *Metrics and Compliance Summary*

As part of the Privacy and Security Program Plan described in section 4.3, metrics are to be identified that provide a measure to the effectiveness of the controls, implementation status, and impact (such as non-compliance). As is the case for most metric collections, measures should result in quantifiable information that is readily obtainable and repeatable. The primary goal of the metrics should be to identify areas of priority and to support appropriate resource allocation for continuous improvement.

Once the DIVS systems are operational, a primary responsibility of the DIVS Program Office is to conduct annual review of VDS compliance. The expectation is that the VDS will develop and maintain a status summary of compliance to the requirements set forth in this document and in

[6] The acceptance process e.g., NIST authorization will be at the discretion of the DIVS Program Office

the DIVS Privacy Policy and DIVS Security Policy. The status summary will not require specific system detail (e.g., details on specific system vulnerabilities), but will focus on the overall implementation of a privacy and security program in alignment with the Framework. The compliance status summary shall be made available to the DIVS Program Office upon request.

REQUIREMENT 10: *The VDS must develop metrics to measure the effectiveness of key controls to assist with decisions for continuous program improvement.*

REQUIREMENT 11: *The VDS agrees to provide the DIVS Program Office with a compliance summary that covers the requirements set forth in this document and the DIVS Privacy and Security Policies.*

Appendix A: Acronyms, Terms and Definitions

Acronym or Term	Definition
Authorization	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls
Availability	Ensuring timely and reliable access to and use of information
Categorization	Categories for information systems based on potential impact on organizations or individuals should there be a breach of security—that is, a loss of privacy / confidentiality, integrity (including authenticity and non-repudiation), or availability.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the privacy / confidentiality, integrity, and availability of the system and its information.
Control Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
DIVS	DL/ID Information Verification Systems
DL/ID	Driver license and/or identification card
FIPS	Federal Information Processing Standards
FISMA (2002)	Federal Information Security Management Act (2002)
FISMA (2014)	Federal Information Security Modernization Act (FISMA) of 2014
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
ISO / IEC 27001	International Organization for Standardization/International Electrotechnical Commission / Information Technology – Security Techniques & Information Security Management Systems - Requirements
NIST	National Institute of Standards and Technology

Acronym or Term	Definition
NIST Special Publications (800 Series)	Special Publications in the 800 series present documents of general interest to the computer security community. The Special Publication 800 series was established in 1990 to provide a separate identity for information technology security publications. This Special Publication 800 series reports on ITL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.
Personally Identifiable Information	Any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual.
PII	Personally Identifiable Information
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
POA&M	Plan of Action and Milestones
Privacy Impact Assessment	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.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
VDS	Vendors, Developers and Suppliers

Appendix B: Summary of Framework Requirements

Framework Component	ID	Framework Document Requirements
General	1	*Each VDS must develop a plan to either implement a privacy and security program OR augment an existing program, to address the intent of the NIST privacy and security controls specified in the Framework. This must be completed and disseminated to the DIVS Program Office within 12 months of contract agreement.*
Governance: Policies and Standards	2	*Each VDS must develop policies that address all NIST control objectives applicable to a **moderate** level information system and include Rules of Behavior ('Acceptable Use Policy').*
	3	*Policy exceptions must be formally documented and approved. Any policy exceptions that may have significant bearing on protecting the privacy / confidentiality, integrity, or availability of the DIVS systems or information must be reviewed and approved by the DIVS Program Office.*
Governance: Senior Management Involvement	4	*A senior management oversight committee is to be established to define organizational privacy and security roles and responsibilities, approve policy and policy exceptions, develop a privacy and security program plan, and ensure that the appropriate privacy and security personnel are assigned for the program.*
Privacy and Security Controls: Procedures and Practices	5	*The VDS must develop procedures or practices to facilitate the implementation of the policy objectives for privacy and each security control family.*
Awareness and Training	6	*The VDS must develop an Awareness and Training plan to address the control objectives defined in policy. Initial focus on awareness and training should be on privacy and the protection of PII.*
Ongoing Risk and Control Assessment	7	*The VDS must incorporate, as part of the privacy and security program, an ongoing process for risk assessment and control assessment. The VDS must conduct initial risk and privacy impact assessments for all DIVS systems for which they have been assigned as owners prior to acceptance in production.*
Employ Continuous Monitoring	8	*The VDS must develop a strategy to ensure that key control areas are continuously monitored for deviation. Various tools can be utilized including configuration management software that identifies and alerts for unplanned changes, data integrity tools, intrusion prevention/detection technologies, and vulnerability scans.*
POA&M for Remediation	9	*The VDS must develop a formal POA&M template to document, in a consistent manner, the tracking of weaknesses ('control gaps') and plans for corrective action.*

Framework Component	ID	Framework Document Requirements
Metrics and Compliance Summary	10	*The VDS must develop metrics to measure the effectiveness of key controls to assist with decisions for continuous program improvement.*
	11	*The VDS agrees to provide the DIVS Program Office with a compliance summary that covers the requirements set forth in this document and the DIVS Privacy and Security Policies.*

Appendix C: Framework Reference Documents – Security Controls

Framework Component	References[7]	Description
Governance: Policies and Standards	DIVS Privacy Policy	All VDS involved in the development, operation, support and use of the DIVS systems shall be required, contractually or via user agreements, to adhere to and implement this policy. *The policy can be used as a basis for the VDS privacy policy or used as a reference to update existing VDS privacy policy.*
	DIVS Security Policy	All VDS involved in the development, operation, support and use of the DIVS systems shall be required, contractually or via user agreements, to adhere to and implement this policy. *The policy can be used as a basis for the VDS security policy or used as a reference to update existing VDS security policy.*
	NIST SP 800-53 Rev. 4 (4/2013)	NIST SP 800-53 provides detail for the controls objectives. - Section 2.2 describes the structure and components of security controls - Appendix D lists and summarizes security control baselines for ***moderate*** information systems - Appendix F documents all security controls, enhancements, and supplemental guidance for each control family
	NIST SP 800-100 (10/2006)	Section 2.2.5, "Information Security Policy and Guidance"
	DIVS Program State-to-State Verification System Requirements Document, Vers. 1.4 (7/2015)	Sections 10.1.1.1 and 10.1.1.2
Governance: Senior Management Involvement	NIST SP 800-53 Rev. 4 (4/2013)	Appendix G, "Information Security Programs"
	NIST SP 800-37 Rev. 1 (2/2010)	Chapter 2, "The Fundamentals" Chapter 3, "The Process – Executing the Risk Management

[7] NIST Special Publications (SP) are located at: http://csrc.nist.gov/publications/PubsSPs.html

Framework Component	References[7]	Description
		Framework Tasks"
	NIST SP 800-100 (10/2006)	Section 2.3, "Information Security Governance Challenges and Keys to Success"
	DIVS Program State-to-State Verification System Requirements Document, Vers. 1.4 (7/2015)	Section 11.1.7, "Privacy and Security Management Plan"

Framework Component	References[8]	Description
ISO 27001 Mapping	NIST SP 800-53 Rev. 4 (4/2013)	Appendix H, "International Information Security Standards," provides a mapping of the NIST security controls to ISO/IEC 27001 This mapping can be utilized for existing VDS programs which are based on ISO/IEC 27001

[8] NIST Special Publications (SP) are located at: http://csrc.nist.gov/publications/PubsSPs.html

Framework Component	References[9]	Description
Security Control: Access Control (AC)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-AC
	NIST SP 800-46 Rev. 1 (6/2009)	*Guide to Enterprise Telework and Remote Access Security*
	DIVS Program State-to-State Verification System Requirements Document, Vers. 1.4 (7/2015)	Section 10.1.1.3
Security Control: Audit and Accountability (AU)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-AU
	NIST SP 800-92 (9/2006)	*Guide to Computer Security Log Management*
	DIVS Program State-to-State Verification System Requirements Document, Vers. 1.4 (7/2015)	Section 9.1, "Auditing" Section 10.1.1.4
Security Control: Configuration Management (CM)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-CM
	NIST SP 800-100 (10/2006)	Section 14, "Configuration Management"
	NIST SP 800-128 (8/2011)	*Guide for Security-Focused Configuration Management of Information Systems*
Security Control: Contingency Planning (CP)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-CP
	NIST SP 800-100 (10/2006)	Section 9, "Information Technology Contingency Planning"
	NIST SP 800-34 Rev. 1 (5/2010)	*Contingency Planning Guide for Federal Information Systems*
	NIST SP 800-84 (9/2006)	*Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
	DIVS Program State-to-State Verification System Requirements Document, Vers. 1.4 (7/2015)	Section 9.4, "Reliability and Availability" Section 9.5, "Fault Tolerance and Recoverability" Section 9.11.1.5 (on "Disaster Recovery documentation and results of periodic testing")

[9] References to control objective detail and procedural references.

Framework Component	References[10]	Description
Security Control: Identification and Authentication (IA)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-IA
	NIST SP 800-63-2 (8/2013)	*Electronic Authentication Guideline*
	NIST SP 800-118 (4/2009)	*Guide to Enterprise Password Management (Draft)*
Security Control: Incident Response (IR)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-IR
	NIST SP 800-100 (10/2006)	Section 13, "Incident Response"
	NIST SP 800-84 (9/2006)	*Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
	NIST SP 800-61 Rev. 2 (8/2012)	*Computer Security Incident Handling Guide*
Security Control: Maintenance (MA)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-MA
Security Control: Media Protection (MP)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-MP
	NIST SP 800-111 (11/2007)	*Guide to Storage Encryption Technologies for End User Devices*
	NIST SP 800-88 Rev. 1 (12/2014)	*Guidelines for Media Sanitization*
Security Control: Physical and Environmental Protection (PE)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-PE
Security Control: Planning (PL)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-PL
	NIST SP 800-18 Rev. 1 (2/2006)	*Guide for Developing Security Plans for Federal Information Systems*

[10] References to control objective detail and procedural references.

Framework Component	References[10]	Description
	NIST SP 800-100 (10/2006)	Section 8, "Security Planning" Section 8.3, "Rules of Behavior"
Security Control: Personnel Security (PS)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-PS

Framework Component	References[11]	Description
Security Control: System and Services Acquisition (SA)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-SA
	NIST SP 800-100 (10/2006)	Section 3, "System Development Life Cycle" Section 5, "Capital Planning and Investment Control"
	NIST SP 800-65 Rev. 1 (7/2009)	*Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process (Draft)*
	NIST SP 800-64 Rev. 2 (10/2008)	*Security Considerations in the System Development Life Cycle*
	NIST SP 800-35 (10/2003)	*Guide to Information Technology Security Services*
	NIST SP 800-36 (10/2003)	*Guide to Selecting Information Technology Security Products*
	NIST SP 800-27 Rev. A (6/2004)	*Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A*
Security Control: System and Communications Protection (SC)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-SC
	NIST SP 800-41 Rev. 1 (9/2009)	*Guidelines on Firewalls and Firewall Policy*
	NIST SP 800-77 (12/2005)	*Guide to IPsec VPNs*
	NIST SP 800-113 (7/2008)	*Guide to SSL VPNs*
	FIPS 140-2 (5/2001)	*Security Requirements for Cryptographic Modules*

[11] References to control objective detail and procedural references.

Framework Component	References[11]	Description
	NIST SP 800-52 Rev 1 (4/2014)	*Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*
	DIVS Program State-to-State Verification System Requirements Document, Vers. 1.4 (7/2015)	Section 10.1.1.6 (on "encryption of sensitive data") Section 10.1.1.7 (on "encryption of all communication links")
Security Control: System and Information Integrity (SI)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-SI
	NIST SP 800-40 Rev. 3 (7/2013)	*Guide to Enterprise Patch Management Technologies*
	NIST SP 800-83 Rev. 1 (7/2013)	*Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
	NIST SP 800-94 (2/2007)	*Guide to Intrusion Detection and Prevention Systems (IDPS)*

Framework Component	References[12]	Description
Security Control: Awareness and Training (AT)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-AT
	NIST SP 800-100 (10/2006)	Section 4, "Awareness and Training"
	NIST SP 800-50 (10/2003)	*Building an Information Technology Security Awareness and Training Program*
	NIST SP 800-122 (4/2010)	*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* – Section 4.1.2 "Awareness, Training, and Education"
Security Controls: Security Assessment and Authorization (CA) Risk Assessment (RA)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-CA Appendix F-RA
	NIST SP 800-53A Rev. 4 (12/2014)	*Assessing Security and Privacy Controls in Federal Information Systems and Organizations:- Building Effective Assessment Plans*
	NIST SP 800-100 (10/2006)	Section 10, "Risk Management" Section 6, "Interconnecting Systems"
	NIST SP 800-37 Rev. 1 (2/2010)	*Guide for Applying the Risk Management Framework to Federal Information Systems*
	NIST SP 800-47 (8/2002)	*Security Guide for Interconnecting Information Technology Systems* – Appendix A "Interconnection Security Agreement"
	FIPS 199 (2/2004)	*Standards for Security Categorization of Federal Information and Information Systems*
	NIST SP 800-30 Rev. 1 (9/2012)	*Guide for Conducting Risk Assessments*
	NIST SP 800-115 (9/2008)	*Technical Guide to Information Security Testing and Assessment*
	NIST SP 800-39 (3/2011)	*Managing Information Security Risk – Organization, Mission, and Information System View*
	NIST SP 800-60 Rev. 1 (8/2008)	*Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories* *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security*

[12] References to control objective detail and procedural references.

Framework Component	References[12]	Description
		Categories
	NIST SP 800-40 Rev. 3 (7/2013)	*Guide to Enterprise Patch Management Technologies*

Framework Component	References[13]	Description
Security Control: Continuous Monitoring (CA) & (RA)	NIST SP 800-37 Rev. 1 (2/2010)	Appendix G, "Continuous Monitoring"
	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-CA Appendix F-RA
	NIST SP 800-100 (10/2006)	Section 2.2.6, "Ongoing Monitoring" Section 11.6, "Continuous Monitoring"
	NIST SP 800-137 (9/2011)	*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
	OMB Memorandum 14-03	*Enhancing the Security of Federal Information and Information Systems*
Security Control: POA&M and Remediation (CA) & (PM)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-CA Appendix G, "Information Security Programs"
	NIST SP 800-37 Rev. 1 (2/2010)	Chapter 3, "The Process – Executing the Risk Management Framework Tasks"
	OMB Memorandum 02-01	"Guidance for Preparing and Submitting Security Plans of Action and Milestones"
Security Control: Metrics and Compliance (CA) & (PM)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix F-CA (Security Assessment Reports) Appendix G, "Information Security Programs"
	NIST SP 800-100 (10/2006)	Section 7 "Performance Measures"
	NIST SP 800-55 Rev. 1 (7/2008)	*Performance Measurement Guide for Information Security*
	DIVS Program Office Compliance Status Report Template	To be provided to the VDS after contract finalization

[13] References to control objective detail and procedural references.

Appendix D: Framework Reference Documents – Privacy Controls

Framework Component	References[14]	Description
Privacy Controls: References to control objective detail and procedural references.		
Privacy Control: General	NIST SP 800-122 (4/2010)	*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
	DIVS Privacy Policy	All VDS involved in the development, operation, support and use of the DIVS systems shall be required, contractually or via user agreements, to adhere to and implement this policy. **Note:** Includes reference to other pertinent Privacy documentation including the DHS *Handbook for Safeguarding Sensitive Personally Identifiable Information* and the *Fair Information Practice Principles (FIPP)*
	NIST SP 800-53 Rev. 4 (4/2013)	Appendix J, "Privacy Control Catalog"
	OMB Memorandum 03-22	"OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002"
	DHS Privacy Impact Assessment Template	http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_template.pdf
	DIVS Program State-to-State Verification System Requirements Document, Vers. 1.4 (7/2015)	Section 11.1.7, "Privacy and Security Management Plan"

[14] NIST Special Publications (SP) are located at: http://csrc.nist.gov/publications/PubsSPs.html

Framework Component	References[15]	Description
Privacy Control Authority and Purpose (AP)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix J, "Privacy Control Catalog"
	The Privacy Act of 1974	§ 552a (e)(3)(A)-(B)
Privacy Control: Accountability, Audit, and Risk Management (AR)	Federal Information Security Modernization Act (FISMA) of 2014	"Subchapter II – Information Security", § 3551
	NIST SP 800-53 Rev. 4 (4/2013)	Appendix J, "Privacy Control Catalog"
	OMB Circular A-130	"Management of Federal Information Resources"
	OMB Memorandum 03-22	"OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002"
	The Privacy Act of 1974	§ 552a
Privacy Control: Data Quality and Integrity (DI)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix J, "Privacy Control Catalog"
	OMB Circular A-130	"Management of Federal Information Resources"
	OMB Memorandum 07-16	"Safeguarding Against and Responding to the Breach of Personally Identifiable Information"
	The Privacy Act of 1974	§ 552a
Privacy Control: Data Minimization and Retention (DM)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix J, "Privacy Control Catalog"
	NIST SP 800-88 Rev. 1 (12/2014	*Guidelines for Media Sanitization*
	NIST SP 800-122 (4/2010)	*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* – Section 4.1.2 "Awareness, Training, and Education"
	OMB Circular A-130	"Management of Federal Information Resources"
	OMB Memorandum 03-22	"OMB Guidance for Implementing the Privacy Provisions

[15] References to control objective detail and procedural references.

Framework Component	References[15]	Description
		of the E-Government Act of 2002"
	OMB Memorandum 07-16	"Safeguarding Against and Responding to the Breach of Personally Identifiable Information"
	The Privacy Act of 1974	§ 552a
Privacy Control: Individual Participation and Redress (IP)	NIST SP 800-53 Rev. 4 (4/2013)	Appendix J, "Privacy Control Catalog"
	OMB Circular A-130	"Management of Federal Information Resources"
	OMB Memorandum 03-22	"OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002"
	The Privacy Act of 1974	§ 552a
Privacy Control: Security (SE)	Federal Information Security Modernization Act (FISMA) of 2014	"Subchapter II – Information Security", § 3551
	FIPS 199 (2/2004)	*Standards for Security Categorization of Federal Information and Information Systems*
	NIST SP 800-37 Rev. 1 (2/2010)	*Guide for Applying the Risk Management Framework to Federal Information Systems*
	NIST SP 800-53 Rev. 4 (4/2013)	Appendix J, "Privacy Control Catalog"
	NIST SP 800-122 (4/2010)	*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* – Section 4.1.2 "Awareness, Training, and Education"
	OMB Circular A-130	"Management of Federal Information Resources"
	OMB Memorandum 03-22	"OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002"
	OMB Memorandum 06-19	"Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments"
	OMB Memorandum 07-16	"Safeguarding Against and Responding to the Breach of Personally Identifiable Information"
	The Privacy Act of 1974	§ 552a

Framework Component	References[15]	Description
Privacy Control: Transparency (TR)	ISE Privacy Guidelines[16]	"Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment"
	NIST SP 800-53 Rev. 4 (4/2013)	Appendix J, "Privacy Control Catalog"
	OMB Circular A-130	"Management of Federal Information Resources"
	OMB Memorandum 03-22	"OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002"
	OMB Memorandum 07-16	"Safeguarding Against and Responding to the Breach of Personally Identifiable Information"
	OMB Memorandum 10-22	"Guidance for Online Use of Web Measurement and Customization Technologies"
	The Privacy Act of 1974	§ 552a
Privacy Control: Use Limitation (UL)	ISE Privacy Guidelines[17]	"Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment"
	NIST SP 800-53 Rev. 4 (4/2013)	Appendix J, "Privacy Control Catalog"
	The Privacy Act of 1974	§ 552a

[16] http://ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf
[17] http://ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf

Attachments: DIVS Policies

DIVS Privacy Policy for Vendors, Developers and Suppliers

DIVS Security Policy for Vendors, Developers and Suppliers