Privacy Impact Assessment

Business Intelligence (BI)

Rural Development (RD)

- February 2018
- Prepared for: RD

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	07/26/2016	ISSS/SN	Transitioned to new template
1.1	02/02/2018	SAC	FY18, updated FOIA Liaison, updated responses

Abstract

Business Intelligence (BI) is a combination of applications which includes ElectroFiche (eFiche), FOCUS, Geospatial Data Warehouse (GDW), Hyperion/Enterprise Performance Management (EPM) 11, Oracle Business Intelligence Foundation Suite (OBIFS), Tableau Reporting System (TRS) and Tabular Data Warehouse (TDW).

BI application's primary purpose provides the capability to enter, maintain, retrieve, and analyze data. It also provides canned reports as well as query and analysis capabilities. BI applications are utilized by USDA employees.

Overview

eFiche is a medium to store, read and retain files for USDA Rural Development (RD). These files are reports generated by UDSA enterprise-level accounting and reporting systems. The eFiche server is a member server in the USDA domain and is accessible at http://eFiche.rural.usda.gov. eFiche produces paper copy reports distributed to Farm Services Agency (FSA), Centralized Servicing Center (CSC), National Financial and Accounting Operations Center (NFAOC), and Deputy Chief Information Officer (DCIO).

FOCUS utilized in producing reports from data residing on the NITC mainframe. FOCUS is capable of providing a complete information control system with comprehensive features for entering, maintaining, retrieving, and analyzing data.

GDW is considered a data mart to the elaborate and complex assortment of servers, networks, storage, data, software and people that logically and physically have been overlaid on existing IT infrastructure and business practices that make up the GDW.

GDW data mart is setup as an RD application for department wide intranet (internal) use only. No public access is available. GDW provides services to intranet based agency applications, and provides its own pre-developed client-server and web browser based access interfaces. This commercially provided non-public mapping and spatial data is then internally coupled to or compiled with certain non-sensitive financial reporting statistics by GDW internal system functions.

Hyperion/EPM11: comprised of a COTS application that provides canned reports as well as query and analysis capabilities using server-side Open Database Connectivity (ODBC) technology for centralized connectivity to a variety of data sources.

OBIFS (formerly Oracle Business Intelligence Enterprise (OBIEE)) is a COTS application that provides canned reports as well as query and analysis capabilities using server-side Open Database Connectivity (ODBC) technology for centralized connectivity to a variety of data sources.

TDW is a repository providing critical business data, in an expedient manner for the

RD decision-makers to sustain their respective program missions. It provides program personnel from the RD major program areas with loans and grants information needed to make sound management decisions supporting the needs of their customers.

TRS is comprised of a COTS application that provides canned reports as well as query and analysis capabilities using server-side Open Database Connectivity (ODBC) technology for centralized connectivity to a variety of data sources. Provides multiple users access to various databases using centralized database connections that have been established on the application server.

NOTE: Per the PTA, GDW and OBIFS are not required to complete the PIA and will not be included in the remainder of this document.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

eFiche:

- The general public
- Name
- Address Information
- Personal identification number
- Financial data
- Miscellaneous identification numbers
- Handwriting or an image of the signature
- SSN/TIN

FOCUS*:*

- USDA employees
- Contractors or other entities working on behalf of USDA
- Name
- Address Information
- SSN/TIN

Hyperion/EPM11

- USDA employees
- Contractors or other entities working on behalf of USDA
- The general public

- Name
- Address Information
- Personal identification number
- Miscellaneous identification numbers
- Handwriting or an image of the signature
- SSN/TIN

TDW:

- The general public
- Name
- Address Information
- Personal identification number
- Financial data
- Miscellaneous identification numbers
- Handwriting or an image of the signature
- SSN/TIN

TRS Employee Information:

- USDA employees
- Contractors or other entities working on behalf of USDA
- The general public
- Name
- Address Information
- Personal identification number
- Financial data
- Miscellaneous identification numbers
- Handwriting or an image of the signature
- SSN/TIN

1.2 What are the sources of the information in the system?

eFiche, FOCUS, Hyperion/EPM11, and TRS: eFiche receives data from NITC mainframe datasets created by the source systems. FSA (PLAS), financial management information to support loan and grant origination and servicing. Information is collected by the system of record - refer to System of Record for USDA loan and grant application, origination and servicing under: LoanServ, Automated Multi-Family Housing Accounting System (AMAS), Program Loan Accounting System (PLAS), Farmer Programs (FP), Community Facilities (CF), Commercial Loan Servicing System (CLSS), Rural Business and Industry (B&I), Water and Environmental Programs (WEP) and Guaranteed Loan System (GLS). Information is then securely extracted from system source data and provided for use by agency staff.

Hyperion: ECM sends information to Hyperion for reports. Hyperion receives data from TDW.

TDW: receives data for reports from: AMAS, CLSS, GLS, LoanServ (DLATS EDI),

MFIS, PFCS, (New Loan Originations) CPAP, RD Apply, and Support Applications (APR), and ACR (eServices).

1.3 Why is the information being collected, used, disseminated, or maintained?

eFiche: Information is being collected for business intelligence purposes and made available to RD employees for business analysis, data trending, data mining, etc.

FOCUS: USDA loan servicing data and USDA financial management needs are supported by information provided for business intelligence purposes.

Hyperion/EPM11: The server information is maintained to provide predefined queries that are submitted to USDA loan servicing data sources and USDA financial management data sources. User account information is processed to support application authorization and reporting.

TDW: Information is being collected for business intelligence purposes and made available to RD employees for business analysis, data trending, data mining, etc. User account information is collected maintained to support application authorization.

TRS: The server information is maintained to provide predefined queries that are submitted to USDA loan servicing data sources and USDA financial management data sources. User account information is processed to support application authorization and reporting.

1.4 How is the information collected?

eFiche, FOCUS: Information is collected by the system of record - refer to System of Record for USDA loan and grant application, origination and servicing under: LoanServ, Automated Multi-Family Housing Accounting System (AMAS), Program Loan Accounting System (PLAS), Farmer Programs (FP), Community Facilities (CF), Commercial Loan Servicing System (CLSS), Rural Business and Industry (B&I), Water and Environmental Programs (WEP) and Guaranteed Loan System (GLS). Information is then securely extracted from system source data and provided for use by agency staff.

Hyperion/EPM11: N/ A , data is not collected, it is processed to provide canned reports as well as query and analysis capabilities using server-side Open Database Connectivity (ODBC) technology.

TDW: Source system data is securely transferred by source systems to data warehouse.

TRS: N/ A , data is not collected, it is processed to provide canned reports as well as query and analysis capabilities using server-side Open Database Connectivity (ODBC) technology.

1.5 How will the information be checked for accuracy?

eFiche, FOCUS, TRS: This is the responsibility of the system of record (SOR). Correct processing and loading of data into reporting systems is monitored by the

Operations Scheduling Branch (OSB).

Hyperion/EPM11: Validation queries are run to compare data loaded into the data warehouse tables to data content within the input flat files.

TDW: Validation queries are run to compare data loaded into the data warehouse tables to data content within the input flat files.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Legal Authority: Rural Development is authorized by the Consolidated Farm and Rural Development Act (7 U.S.C. 1921 et. seq.); and Title V of the Housing Act of 1949, as amended (42 U.S.C. 1471 et. seq.) to solicit the information requested on Rural Development application forms.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

RISK: The risk is in the potential unauthorized disclosure or illegal use of this PII and the potential adverse consequences this disclosure or use would have on the client.

MITIGATION: Data is stored in a secure environment behind the NITC secure mainframe and midrange infrastructure. See the System Security Plan (SSP) security controls Accountability, Audit and Risk Management (AR), Data Quality and Integrity (DI) and Data Minimization and Retention (DM).

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

eFiche: produces Loan servicing and USDA financial management paper copy reports distributed to Farm Services Agency (FSA), Customer Servicing Center (CSC), National Financial and Accounting Operations Center (NFAOC), and Deputy Chief Information Officer (DCIO).

FOCUS: produces reports from Loan servicing and USDA financial management data residing on the NITC mainframe. FOCUS is capable of providing a complete information control system with comprehensive features for entering, maintaining, retrieving, and analyzing data.

Hyperion/EPM11: Hyperion/EPM11 provides canned reports as well as query and analysis capabilities to multiple users. The applications access various databases using centralized database connections that have been established on the application server. Analysts can also use a standalone client to build queries, reports, pivots, charts, and Executive Information System (EIS) dashboards to facilitate navigation and control. Reports and documents are updated via the server's scheduling component.

TDW is a repository providing critical business data, in an expedient manner for the RD decision-makers to sustain their respective program missions. It provides program personnel from the RD major program areas with loans and grants information needed to make sound management decisions supporting the needs of their customers.

TRS: provides multiple users access to various reports and dashboards. TRS supports query and analysis capabilities using pre-defined data sources that allow users to analyze data with intuitive drag and drop capabilities. Tableau features visualized data in minutes and smart dashboards where you can combine multiple views of data. Tableau utilizes live connections along with automatic updates on a schedule.

2.2 What types of tools are used to analyze data and what type of data may be produced?

eFiche: N/A

FOCUS, Hyperion/EPM11: use a software product, Information Builders, Inc. capable of providing complete information control systems with comprehensive features for entering, maintaining, retrieving, and analyzing data. RD's main purpose in utilizing this software is to provide reporting capabilities.

TDW: Hyperion is used to run queries and produce reports against data in data warehouse.

TRS: does not collect, maintain or change public information. TRS reads secure information from legacy data sources to produce read only reports. TRS utilizes analytical, reporting and dashboard presentation tools. TRS produces a wide variety of reports and dashboards. RD's main purpose in utilizing this software is to provide reporting capabilities.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

N/A

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The National Institute of Standards and Technology (NIST) 800-53 controls for BI are discussed in detail in the System Security Plan and specifically the Access Controls (AC 1-6, 11, 12, 14, 17, 20, and 21), Identification and Authentication (IA 1-8) controls are in place to prevent unauthorized access restricting users from accessing the operating system, other applications or other system resources not needed in the performance of their duties and is restricted by eAuthentication (eAuth). The Authority and Purpose (AP 1-2) compensating controls give explanation of why PII is allowed on the system. Systems and Communication Protection (SC 1, 2, 4, 5, 7, 8, 10, 12, 13, 17, 20-23, 28, and 39) controls are in place to prevent unauthorized access.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

EFiche, FOCUS: Life of the loan.

Hyperion/EPM11, TRS: The data only passed through the system. It is not retained. User access information is retained as long as it is required to provide users access to the system. Applications (.bqy files) are maintained until they are replaced or removed by the publisher.

TDW: Information is retained for the last three years of monthly snapshots, and end of calendar year and end of fiscal year snapshots for the fourth and fifth years are retained.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes, the System of Record (SOR) was completed and submitted to NARA in accordance with Section 207 (e) of the E-Government Act of 2002 [44 U.S.C. 3601] and NARA Bulletins 2008-03, *Scheduling Existing Electronic Records*, and 2006-02, *NARA Guidance for Implementing Section 207(e) of the E-Government Act of 2002.*

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

RISK: Information being retained for various indeterminate lengths of time (life of loan, pass through, etc.) can potentially be a risk. With data stored for various lengths of time there is the potential of unauthorized access, unauthorized disclosure or illegal use of the customer PII data.

eFiche, FOCUS: The risk is retaining data for the life of the loan.

Hyperion/EPM11, TDW, TRS: Risk is the retention of reports as long as an approved user wishes to keep the data. The user of these reports are approved RD employees who are trained and instructed in the methods of securing RD data.

MITIGATION: Data Integrity controls (DI 1-2) are used to protect data from accidental or malicious alteration and destruction providing assurance to the user the information meets expectations for quality and it has not been altered. Validation controls refer to tests and evaluations used to determine compliance with security specifications and requirements are in place. Methods such as overwriting the entire media, degausses, and disk formatting are used, but strict attention is paid to whatever process is selected to ensure that all unneeded data is completely destroyed. Papers and other soft materials, such as microfiche and CD's, are shredded. Also, the data is stored in a secure environment behind the NITC secure mainframe infrastructure. See the System Security Plan (SSP) security controls Accountability, Audit and Risk Management (AR), Data Quality and Integrity (DI) and Data Minimization and

Retention (DM).

TDW: Risk is mitigated by retaining the last three years of monthly snapshots, end of calendar year and end of fiscal year snapshots for the fourth and fifth years.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

eFiche, FOCUS, Hyperion/EPM11, TDW, and TRS: FSA (PLAS), financial management information to support loan and grant origination and servicing and for business analysis, data trending, data mining, etc.

Hyperion: ECM sends information to Hyperion for reports. Hyperion receives data from TDW. The server information is maintained to provide predefined queries that are submitted to USDA loan servicing data sources and USDA financial management data sources. User account information is collected maintained to support application authorization.

TDW: receives data for reports from: AMAS, CLSS, GLS, LoanServ (DLATS EDI), MFIS, PFCS, (New Loan Originations) CPAP, and RD Apply, and Support Applications (APR), and ACR (eServices). Information is being collected for business intelligence purposes and made available to RD employees for business analysis, data trending, data mining, etc. User account information is collected maintained to support application authorization.

4.2 How is the information transmitted or disclosed?

eFiche, FOCUS, Hyperion/EPM11, TDW and TRS: Electronically, PDF, XLS and encrypted data files.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

RISK: The risk to internal information sharing would be the unauthorized disclosure of lender status and loan closing reports, obligation and disbursement data, statement and tax report information, borrower information and accounting information.

MITIGATION: The NIST 800-53 controls are discussed in the SSP. System and Communication Protection (SC) to prevent unauthorized and unintended information transfer. System and Integrity (SI) controls are in place to provide integrity and confidentiality. The security and control of PII is the responsibility of the System Owner and RD employees. Risk is mitigated with the implementation of RD ISSS NIST policies, standards and procedures. Also, the data is stored in a secure environment behind the NITC secure mainframe infrastructure.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

No information is shared outside the department.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

No information is shared outside the department.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

No information is shared outside the department.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

No information is shared outside the department.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

Yes, USDA/Rural Development-1 Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and Other Participants in RD Programs (http://www.ocio.usda.gov/policy-directives-records-forms/records-management/system-records).

6.2 Was notice provided to the individual prior to collection of information?

N/A: Since the data is not collected directly from the individual, this question is only applicable to the SOR.

6.3 Do individuals have the opportunity and/or right to decline to provide information?

NA

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

NA

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

NA, Individual do not have direct access to the system. Individuals have the option to decline to proceed. If the user declines, no data is collected; therefore, no risk is associated. If the user accepts, they provide their own data, to the SOR, and are aware of the information being collected.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

BI systems do not allow external users. If data is incorrect for a borrower, it is addressed by the SOR.

7.2 What are the procedures for correcting inaccurate or erroneous information?

BI systems do not allow external users. If data is incorrect for a borrower, it is addressed by the SOR.

Formal requests for correction of USDA information must be submitted by letter, fax, or e-mail to the Information Quality Official(s) of the USDA agency or office that disseminated the information (henceforth in these procedures, the term "USDA agency" shall mean "USDA agency or office"). For requests for correction concerning information on which USDA seeks public comment, submit the correction request during the comment period.

After the responsible USDA agency has made its final determination pertaining to a request for correction of information, that agency will respond to the requestor in writing by letter, e-mail, or fax, normally within 60 calendar days of receipt. The response will explain the findings and the actions the agency will take (if any) in response to the complaint.

If the request requires more than 60 calendar days to resolve, the agency will inform the complainant within that time period that more time is required, and the reasons for the

delay, and an estimated decision date.

Customers and employees may contact the Freedom of Information Officer:

Joseph Shunk
FOIA Liaison
1400 Independence Ave., SW
Stop 0706
Washington, DC 20250-0706
Tel. 202-690-5394
Email: ssd.FOIA@wdc.usda.gov

7.3 How are individuals notified of the procedures for correcting their information?

BI systems do not allow external users. If data is incorrect for a borrower, it is addressed by the SOR.

7.4 If no formal redress is provided, what alternatives are available to the individual?

BI systems do not allow external users. If data is incorrect for a borrower, it is addressed by the SOR. Also, individuals have access, redress, and amendment rights under the Privacy Act and the Freedom of Information Act.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

No additional risks are associated with the redress process.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

Generally, the National Institute of Standards and Technology (NIST) 800-53 security controls are detailed in the System Security Plan and specifically the Access Control (AC), Identification and Authentication (IA) and Systems and Communication Protection (SC) controls are in place to prevent unauthorized access. Access control is also addressed in the individual systems desk procedures.

Desk Procedures document the User Access Management (UAM) process for establishing, activating, and modifying IDs. This process is defined by System Owners. System Owners define Groups and account types. System Point of Contact assigns group membership and determines Need-to-Know validation. The POC is responsible for verifying the user's identification; the UAM Team relies on a POC supplying the correct UserID and password. UAM is tool used to create, modify and delete user

requests approved the System Point of Contact (POC).

8.2 Will Department contractors have access to the system?

Yes

8.3 8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

USDA RD requires annual Information Security Awareness Training (ISAT) for all employees and contractors. RD is responsible for ensuring all new employees and contractors have taken the Department Security Awareness Training developed by OCIO-CS. Training must be completed with a passing score prior to access to a USDA RD system.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes, the current ATO is valid until 27 January 2020.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

RD has an Audit and Accountability Policy, Standards, and Procedure that defines the following auditable events: server startup and shutdown, loading and unloading of services, installation and removal of software, system alerts and error messages, user logon and logoff attempts (both successful and unsuccessful), granting of elevated privileges (root access success and failure), modifications of privileges and access controls, all root commands (success and failure), and sensitive files accessed, modified and added. These controls, including full compliance, inheritance, and risk acceptance descriptions, are available in CSAM.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

RISK: There is minimal risk given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system.

MITIGATION: However, RD has the following controls in place - collecting auditable events: date and time of the event, the component of the information system where the event occurred, type of event, user/subject identity, and the outcome (success or failure) of the event. Audit logs will be reviewed by the NITC Security Division every two weeks and suspicious activity will be investigated. Suspicious activity includes, but not limited to: modifications or granting of privileges and access controls without proper request submitted, consecutive unsuccessful log-on attempts that result in a user being locked, multiple unsuccessful log-on attempts without lock out by the same User Identification

(UserID), modifications or attempted modification of sensitive files without authorization and within the applications repeated attempts to access data outside a user's privilege.

Per the General Records Schedules, (https://www.archives.gov/records-mgmt/grs.html), the following items will be deleted/ destroyed when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes: electronic files and hard copy printouts created to monitor system usage, including, but not limited to, log-in files, password files, audit trail files, system usage files, and cost-back files used to assess charges for system usage.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

This project is part of the Comprehensive Loan Program (CLP) Investment and facilitates the processing by USDA personnel of applications, obligations, loans, grants, and collections on behalf of RD Commercial Program customers.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

BI does not raise any privacy concerns because of its employed technology.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 *"Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?*

Yes, guidance has been reviewed by all parties.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

Although GDW is not included in this PIA, GDW as a part of Business Intelligence, does use a third party website for address validations.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

BI does not use third party websites or applications.

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

BI does not use third party websites or applications.

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

BI does not use third party websites or applications.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

BI does not use third party websites or applications.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

BI does not use third party websites or applications.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

BI does not use third party websites or applications.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

BI does not use third party websites or applications.

10.10 Does the system use web measurement and customization technology?

BI does not use web measurement and customization technology.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

BI does not use web measurement and customization technology.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

BI does not use third party websites or applications.

Responsible Officials

GREG ESCHMAN

Digitally signed by GREG ESCHMAN
Date: 2018.03.23 10:39:56 -05'00'

Greg Eschman
Director, TSSCD

Approval Signature

DIEGO MALDONADO

Digitally signed by DIEGO MALDONADO
Date: 2018.03.30 06:59:16 -05'00'

Diego Maldonado
Chief Information Security Officer (CISO) & Privacy Officer