

FOR OFFICIAL USE ONLY



FEMA

Memorandum of Understanding
between
NFIP Information Technology Services
and
WYO Company

Version 5.6

November 16, 2007

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid “need-to-know” without prior approval of the **FEMA NFIP IT Services** and **WYO COMPANY** Disclosure Offices.

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	November 16, 2006	Initial Template Creation – Alisha Johnson
1.1	December 18, 2006	Incorporated the Topological Drawing – Alisha Johnson
1.2	December 21, 2006	Modifications – Bruce A. Legatie
1.3	June 29, 2007	CISO Update with Components’ Recommended changes in Sections 1.0, 1.3, 1.4, 1.5, 2.0, 3.1, 3.2, 3.4, 3.6, 3.7, 3.8, 3.9, 3.12, 3.13, 3.18, 4.0, 5.0, Attachment A, Attachment B. Created section 3.10 Formal Security Policy.
1.4	August 2, 2007	CISO Update with Components’ Recommended Changes for Sections: 1.1, 1.2, 1.5, 3.17, 3.2, 5.0. Annotated Component POCs in all sections noted in version 1.3 where recommended changes were inserted.
1.5	September 10, 2007	FLETC and CISO comments
5.5	September 30, 2007	Minor editorial changes. Updated date and version number to coincide with current Handbook.
5.6	November 16, 2007	Customization for the National Flood Insurance Program – Jack Way, NFIP ISSO

FOR OFFICIAL USE ONLY

CONTENTS

1.0 PURPOSE.....2

1.1 Security Network Connectivity Policy2

1.2 MOU Requirements for Types of System Interconnections.....2

1.3 Scope.....3

1.4 Point of Contact (POC).....3

1.5 References.....3

2.0 INTERCONNECTION STATEMENT OF REQUIREMENTS.....4

3.0 SECURITY CONSIDERATIONS4

3.1 General Information/Data Description5

3.2 MOU Requirements Within and Across Organizational Boundaries.....5

3.3 Physical Security and Environmental Controls5

3.4 Data Sensitivity.....5

3.5 Services Offered.....6

3.6 Period of Operation.....7

3.7 User Community.....7

3.8 Information Exchange Security9

3.9 Trusted Behavior / Rules of Behavior9

3.10 Formal Security Policy9

3.11 Incident Reporting9

3.11.1 System Monitoring.....10

3.12 Security Audit Trail Responsibility10

3.13 Specific Equipment/Service Restrictions.....11

3.14 Dial-Up/Remote Connectivity.....11

3.15 Training and Awareness11

3.16 Security Documentation.....11

3.17 Change Control12

4.0 TOPOLOGICAL DRAWING13

5.0 SIGNATORY AUTHORITY.....14

FOR OFFICIAL USE ONLY

1.0 PURPOSE

This Memorandum of Understanding (MOU) is required by Federal and Department of Homeland Security (DHS) policy and establishes individual and organizational security responsibilities for the protection and handling of unclassified information between the **FEMA NFIP Information Technology (IT) Services** and the **WYO Company**. Any specific requirements of both signatory organizations are also included.

1.1 Security Network Connectivity Policy

DHS Sensitive Systems Policy Directive 4300A establishes DHS policy for network connectivity. The section on network connectivity (Section 5.4.3) states:

- a. Components shall ensure appropriate identification and authentication controls, audit logging, and access controls are implemented on every network component.
- b. Interconnections between sensitive IT systems and IT systems not controlled by the DHS shall be established only through controlled interfaces. The controlled interfaces shall be accredited at the highest security level of information on the network.
- c. MOUs shall be reissued every three years or whenever any significant changes have been made to any of the interconnected systems.
- d. MOUs shall be reviewed as a part of the annual FISMA self-assessment.

1.2 MOU Requirements for Types of System Interconnections

System interconnections may be characterized as either direct or networked. Direct connections are single purpose point-to-point connections that support only the two connected systems. Directly connected systems do not rely on another network for their connectivity or security and are physically and electronically isolated from other networks and systems. Networked systems connect via an intervening network that exists as a general support system, not a single-purpose connection. Systems that are connected via an encrypted tunnel, whether on HSDN or any other network, are considered networked systems.

For networked U.S. Government systems, the MOU must include the owner and DAA of the network as well as the owners of the applicable systems.

The NFIP IT Services and WYO Companies interconnection is considered a networked connection by virtue of the Transaction Record Reporting Process (TRRP) and supporting required applications. This MOU is intended to recognize the relationship between DHS FEMA NFIP IT Services and a NFIP Write-Your-Own Insurance (WYO) Company and is subordinate to Article II of The Write Your Own Financial Assistance/Subsidy Arrangement (Arrangement).¹ For WYO Companies that engage a flood systems vendor(s) (Vendor), the MOU identifies each company's vendor in conjunction with a technically oriented Interconnection Security Agreement (ISA) that is established between NFIP IT Services and the Vendor. For WYO

¹ The Financial Assistance/Subsidy Arrangement, Appendix A to Part 62, Effective October 1, 2005

FOR OFFICIAL USE ONLY

Companies that process their own data, the WYO will have only an ISA established with FEMA NFIP IT Services.

1.3 Scope

This memorandum of understanding addresses the interaction of the *FEMA Mitigation Directorate NFIP IT Services* and the *WYO Company*. *WYO Company* engages *Vendor Name* to support NFIP transaction processing including TRRP submissions.

1.4 Point of Contact (POC)

For all issues associated with this agreement, the established points of contact are as follows:

Designated Accrediting Authority (DAA) (Comparable WYO/Vendor Position)

Information Systems Security Officer (ISSO) (Comparable WYO/Vendor Position)

Information Systems Security Manager (ISSM) (Comparable WYO/Vendor Position)

<i>FEMA Mitigation Directorate NFIP Operations</i>	<i>WYO Company or Vendor</i>
DAA: David Maurstad or Ed Connor	DAA:
System Owner: David Maurstad or Ed Connor	System Owner:
ISSO(s): Jack Way	ISSO(s):
Program Manager: Laurie Michie	Program Manager

1.5 References

NIST Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Technology Systems*, provides guidance in preparing and establishing connectivity between networks. SP 800-47 specifies guidance for establishing network MOUs. The key points are discussed in this MOU. Referenced documents are available to WYO Companies and vendors upon request to the ISSO.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines apply to all components of an information system that process, store, or transmit federal information.

- DHS Sensitive Systems Policy Directive 4300A
- DHS 4300A Sensitive Systems Handbook
- DHS, Type Accreditation, Attachment D to the DHS 4300A Sensitive Systems Handbook
- DHS, Incident Response and Reporting, Attachment F to the DHS 4300A Sensitive Systems Handbook

FOR OFFICIAL USE ONLY

- DHS, Vulnerability Assessment Program, Attachment O to the DHS 4300A Sensitive Systems Handbook
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002
- NIST ITL Bulletin,, Secure Interconnections for Information Technology Systems, February 2003
- NIST SP 800-53, Rev. 1, Recommended Security Controls for Federal Information Systems, December 2006.

2.0 INTERCONNECTION STATEMENT OF REQUIREMENTS.

The signing of an MOU by FEMA and a NFIP Write Your Own (WYO) Company is requisite to identifying a NFIP Insurance Services Vendor to perform the Transaction Record Reporting Process (TRRP) on behalf of a WYO Company or utilizing NFIP IT (NextGen) “A la Carte” or “Core” applications.

This MOU compliments an accompanying ISA which defines the technical responsibilities for establishing, operating and securing a connection to conduct NFIP business transactions. For WYO Companies, the MOU is subordinate to Article II of The Write Your Own Financial Assistance/Subsidy Arrangement (Arrangement)² and are intended to only identify the WYO Company’s vendor and to agree to manage WYO Company personnel that utilized NFIP IT Services’ “A la Carte” or “Core” applications.

The MOU is intended primarily for WYO Companies that rely upon NFIP Insurance Vendors for consolidating and reporting WYO Companies’ NFIP transaction data (TRRP) to FEMA. The MOU is intended for WYO insurance companies’ NFIP business units, to communicate IT systems related expectations with FEMA. In cases where a WYO company performs its own data processing and submissions, the WYO will establish an ISA with FEMA’s NFIP IT Services.

NFIP Insurance Systems Vendors (Vendors) are responsible for establishing an MOU with FEMA’s NFIP IT Services to ensure formal services expectations are established and maintained. WYO companies will acknowledge their insurance systems vendors within their MOUs with FEMA NFIP IT Services. WYO companies will decide whether or not to share their MOUs with their respective vendors.

3.0 SECURITY CONSIDERATIONS

This section describes the security mechanisms in place to secure the connections between both systems. It outlines what the security considerations are and which organization is responsible for each. In some cases both organizations will share security responsibility.

² The Financial Assistance/Subsidy Arrangement, Appendix A to Part 62, Effective October 1, 2005

FOR OFFICIAL USE ONLY

3.1 General Information/Data Description

FEMA NFIP IT Services will provide referential information to support accurate insurance business transactions within the bounds of privacy and NFIP business rules. For example, proper NFIP underwriting practices and NFIP rules require previous claims information to be made available to a prospective policy holder prior to purchase. Complete information requirements are documented within the “Transaction Record Reporting and Processing (TRRP) Plan - Revision 4 including changes through May 2006.” The TRRP plan is available at the following address.

<http://bsa.nfipstat.com/manuals/manuals.htm>

Per the TRRP Plan, **WYO COMPANY NAME through its VENDOR** will provide TRRP and Financial Control Plans will be referenced as the minimum amount of data per WYO Company.

3.2 MOU Requirements Within and Across Organizational Boundaries

IT equipment within the boundary of the **FEMA NFIP IT Systems** is owned, operated and maintained by **FEMA Mitigation Directorate** contracted services or government employees. All **FEMA Mitigation Directorate NFIP** IT equipment interconnected with the **[WYO Company or Vendor System Name]** will be hardened, at a minimum, per DHS MD4300A hardening guidelines or specific waivers to hardening guidelines requested, documented, and approved by appropriate ISSM

IT equipment within the boundary of the **[WYO Company or Vendor System Name]** is owned, operated and maintained by **[WYO Company or Vendor]** contracted services or employees. All **[WYO Company or Vendor System Name]** IT equipment interconnected with the **FEMA NFIP IT Systems** will be hardened, at a minimum, to a comparable level to DHS 4300 hardening guidelines or per specific waivers to hardening guidelines requested, documented, and approved by the NFIP ISSO. (Hardening documentation may be requested from the NFIP IT ISSO.)

FEMA NFIP IT Services and the **[WYO Company or Vendor]** shall protect the data in order to maintain confidentiality, integrity, and availability of the data and information systems. The data and information systems will be protected in accordance with DHS Sensitive Systems Policy Directive MD4300A, the NIST SP 800-53 assigned minimum security controls, and FIPS 199 Security Categorization of both systems to ensure that the connection will be protected to the requirements of higher categorized system.

3.3 Physical Security and Environmental Controls

FEMA NFIP IT Production Systems are physically located at the FEMA Map Service Center (MSC) in Elkridge, Maryland. MSC facilities are certified and accredited per the DHS 4300A Sensitive Systems Policy Section 4.2 “IT Physical Security,” and NIST SP 800-53 controls. Both organizations’ shall provide physical security and system environmental safeguards adequate to provide protection of the system components.

3.4 Data Sensitivity

The highest level of data that traverses the **FEMA NFIP IT Systems** is Sensitive but Unclassified (SBU). This may include, but is not limited to, Sensitive Personally Identifiable

FOR OFFICIAL USE ONLY

Information (PII), For Official Use Only, and NFIP policy or claims transaction financial information.

The highest level of data that traverses the *[WYO Company or Vendor System Name]* is Sensitive but Unclassified (SBU). This may include, but is not limited to, Sensitive Personally Identifiable Information, For Official Use Only, and NFIP policy or claims transaction financial information.

3.5 Services Offered

The interconnection between *FEMA NFIP IT Systems* and the *[WYO Company or Vendor System Name]* is supported by Secure File Transfer Protocol (SFTP), Public Key Infrastructure (PKI) and Secure Socket Layer (SSL) technologies. *FEMA NFIP IT Systems* provides referential information to support accurate insurance business transactions within the bounds of privacy and NFIP business rules to the *[WYO Company or Vendor System Name]*

Services and ports that are needed to access the Department systems are provided on an as-needed basis, in person to protect the integrity of the connection. The table below identifies the NFIP IT (NextGen) applications and transmission methods that will be used to conduct NFIP business by the WYO Company or Vendor identified in this agreement. Required applications are highlighted in red.

Figure C.2-1 NextGen Stakeholder Interaction Frequency and Methods

NextGen Application	Stakeholder Involvement			Frequency	Transmission Methods		
	WYO Companies/Vendors	States, Communities, Regions	NFIP Bureau/Contractors		Real-Time Person-to-Machine	Batch Machine-to-Machine	Web Services Machine-to-Machine
NextGen Daily TRRP	Required ☹️	None	Required	Daily	⊖	⊕	⊖
NextGen Portal	★	★	★	As Needed	⊕	⊖	⊖
Location Validation	Optional	Optional	Optional	As Needed	⊕	⊕	⊕
SQANet	Optional	Optional	Optional	As Needed	⊕	⊖	⊖
Forms	Optional	Optional	Optional	As Needed	⊕	⊖	⊖
Flood Rating Engine Environment (FREE)	Optional ☹️ SFR ONLY	None	Optional	As Needed	⊕	⊕	⊕
Flood Financial Management (F2M)	Required ☹️	None	Required	Monthly	⊕	⊕	⊖
EZClaims	Required ☹️	Optional	Required	Weekly	⊕	⊕	⊖
Company Profile	Required ☹️	None	Required	Minimum Yearly, As Needed	⊕	⊖	⊖
Admin Console	Optional	Optional	Required	As Needed	⊕	⊖	⊖
AW-501	None	Required	Required	As Needed	⊕	⊖	⊖

★ The NextGen portal is optional, however it serves as the gateway to other NextGen applications.

⊕ YES ⊖ NO

The **WYO COMPANY or VENDOR** will use the following applications. (Double Click on Check Boxes)

FOR OFFICIAL USE ONLY

- NG Daily TRRP
- Flood Rating Engine Environment (FREE) for Submit for Rating (SFR)
- Flood Financial Management F2M
- EZClaims
- Company Profile
- Location Validation
- SQANet
- Forms
- Admin Console

3.6 Period of Operation

Both systems are operational 24 hours a day, 7 days a week. TRRP submissions are required on normal business days excluding federal holidays.

3.7 User Community

The user community is comprised of **FEMA NFIP IT** and [**WYO Company or Vendor**] contract and employees. Additionally, other users may include employees or contract employees of other DHS Components and other Federal or State agencies. All users of both systems will have appropriately adjudicated suitability background investigations. Non-US citizens that have access to FEMA NFIP IT Systems are considered appropriate exceptions and will be documented in accordance with DHS Policy.

Under normal conditions, only U.S. Citizens are allowed access to DHS systems and networks, however, at times there is a need to grant access to foreign nationals. In the case of NFIP IT Services, IT support contractors may include foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to appropriate policies are treated separately from standard exceptions and waivers. The approval chain for an exception to the U.S. Citizenship requirement flows through the Component Head, the Office of Security, and the Chief Information Officer. Attachment J to the DHS 4300A Sensitive Systems Handbook provides an electronic form for requesting exceptions to the U.S. Citizenship requirement.

The use of contractors is essential to the success of the NFIP IT Services. Contractors fill a vital role in the daily operations of the Program. They have a responsibility to protect the information they possess and process. To ensure the security of the information in their charge, contractors must adhere to the same rules and regulations as Government employees.

All personnel accessing NFIP IT systems are required to have an appropriate security clearance and a valid need to know in order to access these systems. All FEMA and Contractor employees must have favorably adjudicated background investigations commensurate with the defined sensitivity level of the positions they hold. Determining the appropriate position sensitivity level is based on such factors as the type and degree of harm (e.g., disclosure of sensitive information,

FOR OFFICIAL USE ONLY

interruption of critical processing, computer fraud) the individual can cause through misuse of the computer system.

Additionally FEMA ensures that individuals who support NFIP IT Systems are highly qualified technically and are adequately trained for the position they occupy. This reduces the risk of unintentional actions.

The following table summarizes the user community that will be served by this interconnection, including their approved access levels and the lowest approval level of any individual who will have access to the data resulting from the interconnection.

Organization	Position	Role	Access Level	Capability	Applications	
Public	Citizen	Information Seeker	No Sign In	View Public Data	NFIPNextGen.com	
					Location Validation	
FEMA	NFIP Overseer	Underwriting Specialist	Sign In Required	View WYO Company Data	NFIPNextGen.com	
		Claims Specialist	Sign In Required	View WYO Company Data	Location Validation	
					FREE	
					SQANet	
					ezClaims	
		Mitigation Specialist	Sign In Required	View WYO Company Data	SQANet	
					Location Validation	
					ezClaims	
		Actuary	Sign In Required	View WYO Company Data	SQANet	
		IT Monitor & ISSO	Sign In Required	View WYO Company Data	Location Validation	
				Test Tools	FREE	
					SQANet	
					ezClaims	
		Financial Monitor			F2M	
				TRRP		
		Regional NFIP Coordinator	Sign In Required	View WYO Company Data	SQANet	
	Disaster Assistance Employee	Field Disaster Assistance Provider	Sign In Required	View WYO Company Data	SQANet	
FEMA Contractors	NFIP IT Programmer Analyst	Updates and Repairs Programmer	Sign In Required	View WYO Company Data	Information Systems Support	
	NFIP IV&V Analyst	Systems Tester	Sign In Required	View WYO Company Data	FREE	
	NFIP Data Quality Analyst	Data Analyst	Sign In Required	View WYO Company Data	SQANet	
					ezClaims	
					F2M	
					TRRP	
					FREE	
		NFIP Underwriting Support	Underwriter			Location Validation
						SQANet
		NFIP Claims Support	Claims Analyst Claims General Adjuster			ezClaims Location Validation
					SQANet	
	NFIP Financial Support	Financial Analyst			F2M	
					SQANet	
	NFIP Actuarial Support	Actuarial Analyst			SQANet	
	NFIP Management Support	Program/Project Manager	Sign In Required	View WYO Company Data	SQANet	
	NFIP Business Analysts	WYO Company and Vendor Liaison	Sign In Required	View WYO Company Data	Admin Console	
			Sign In Required	View WYO Company Data	WYO Company/Vendor Profile	
			Sign In Required	View WYO Company Data	SQANet	
State	State Employee	State NFIP Coordinator	Sign In Required	View WYO Company Data	SQANet	
		State Hazard Mitigation Officer	Sign In Required	View WYO Company Data	SQANet	
		NFIP Community Coordinator	Sign In Required	View WYO Company Data	SQANet	
Communities WYO Insurance Company	Municiple, Regional, County Employee					
		Flood Director or Delegate	Flood Business Director	Sign In Required	View WYO Company Data	SQANet
				Sign In Required	View WYO Company Data	WYO Company/Vendor Profile
		Underwriting Specialist	Underwriter	Sign In Required	View WYO Company Data	SQANet
						Location Validation
				Sign In Required	View WYO Company Data	FREE
		NFIP Claims Specialist	Claims Analyst/Adjusters	Sign In Required	View WYO Company Data	SQANet
						Location Validation
				Sign In Required	View WYO Company Data	ezClaims
		WYO Financial Management	Flood Financial Analysts	Sign In Required	View WYO Company Data	F2M
		IT Administrator	TRRP Submission Coordinator	Sign In Required	View WYO Company Data	SQANet
				Sign In Required	View WYO Company Data	TRRP
				Sign In Required	View WYO Company Data	Admin Console
	WYO Insurance Vendor	NFIP Director or Delegate	Flood Business Director	Sign In Required	View WYO Company Data	SQANet
				Sign In Required	View WYO Company Data	WYO Company/Vendor Profile
		Underwriting Specialist	Underwriter	Sign In Required	View WYO Company Data	SQANet
						Location Validation
				Sign In Required	View WYO Company Data	FREE
		NFIP Claims Specialist	Claims Analyst/Adjusters	Sign In Required	View WYO Company Data	SQANet
						Location Validation
				Sign In Required	View WYO Company Data	ezClaims
		NFIP Financial Management	Flood Financial Analysts	Sign In Required	View WYO Company Data	F2M
		IT Administrator	TRRP Submission Coordinator	Sign In Required	View WYO Company Data	SQANet
			Sign In Required	View WYO Company Data	Admin Console	
			Sign In Required	View WYO Company Data	TRRP	

3.8 Information Exchange Security

Both organizations will ensure that virus and spyware detection and eradication capabilities are used where appropriate (e.g., workstations, laptops, servers, etc.) and that adequate system access controls are in place and maintained on all components connected to the systems. FEMA NFIP IT Systems utilize the following commercial off the shelf (COTS) technologies for maintaining systems security.

- FPROT Antivirus Software for Unix Servers
- Computer Associates Site Minder and Identity Manager access control software
- PGP PKI 128 byte encryption software
- Verisign Secure Socket Layer software

Specific protocols and ports that are needed to support this interconnection are provided on a case-by-case basis, as needed.

3.9 Trusted Behavior / Rules of Behavior

The *FEMA NFIP IT Systems* users and *[WYO Company]* users, to include system administrators, are expected to protect data in accordance with the policies, standards, and regulations specified for each system. This includes *DHS FEMA* and *[WYO Company]* policy and the documented rules of behavior for each system. The following documents specify specific rules of behavior for each system:

FEMA NFIP IT Systems: DHS 4300 A, Sensitive Systems Handbook, Attachment G, Rules of Behavior, Version 5.0, March 2007

All FEMA NFIP IT Services Contractors and FEMA employees working directly with NFIP insurance data are expected to sign the General Rules of Behavior Acknowledgement form.

[WYO Company or Vendor]: Document Name. If no document exists please state there is no formal rules of behavior documentation at this time.

3.10 Formal Security Policy

Policy documents that govern the protection of the data between the two organizations systems are: *DHS – FEMA Sensitive Systems Policy, Directive 4300A, Version 4.2, September 29, 2006* and *[WYO Company] [Policy Name] [Policy Date]*.

3.11 Incident Reporting

The organization discovering a security incident will report it in accordance with the organization's incident reporting procedures and ensure that the other connecting organization is notified. *FEMA NFIP IT government and contractor personnel* shall report security incidents to the FEMA Helpdesk and DHS Security Operations Center (SOC). FEMA Help Desk and DHS SOC contact information is below:

FEMA-National Help Desk: FEMA-NationalHelpdesk@dhs.gov, (540) 542-4000

FOR OFFICIAL USE ONLY

DHS 1NET Support: 1-877-DHS1NET or 1-877-347-1638
Option 1 = NOC
Option 2 = SOC

DHS SOC Direct Line: (703) 921-6505

FEMA NFIP IT personnel (government and contractors) will be notified of any security incident that may have an operational or security impact on the **FEMA NFIP IT Systems** resources. Likewise, the **[WYO Company]** POC shall be notified of any security incident that may have an operational or security impact on **[WYO Company or Vendor System Name]** connected to **FEMA NFIP IT Systems**. More detail regarding FEMA management of IT security incidents is provided in Attachment B as it appears in FEMA Standard Operating Procedure 1540#1, July 10, 2006.

3.11.1 System Monitoring

The **FEMA NFIP IT Systems** performance and operations are monitored and managed using generic Solaris scripts and all NFIP IT servers are installed with a client utility called NetConnect, which collects and maintains system information and provides a management Web interface at <https://srsnetconnect.sun.com>. For the Windows portions of NFIP IT Architecture, FEMA has adopted Dell OpenManage IT Assistant (DOMITA) to conduct its Microsoft Windows server monitoring. DOMITA provides a centralized management console that connects to agent controllers on each Dell server. The agents send detailed information to the console to enable pro-active alerting and real-time monitoring of the health of each server.

FEMA NFIP IT is deploying and using the products listed in section 3.8 and their built-in capabilities to monitor security vulnerabilities and compliance: Specific protocols and ports that are needed to support this interconnection are provided on a case-by-case basis, as needed.

The **[WYO Company]** performance and operations are monitored and managed using the following products and tools:

List the tools

[WYO Company] is deploying and/or using the following products and capabilities to monitor security vulnerabilities and compliance:

List the tools

3.12 Security Audit Trail Responsibility

NFIP IT and WYO Companies and Vendors that interact as described in the ISA are responsible for auditing system security events and user activities involving the interconnection. Activities that will be recorded include:

FOR OFFICIAL USE ONLY

- Event type
- Date and time of event
- User identification
- Server identification
- Success or failure of access attempts
- Security actions taken by system administrators or ISSOs.

Audit logs will be retained for 90 days on-line and available for at least one (1) year (as long as the entries do not contain PII).

NFIP IT Services uses the following products to produce audit logs that are stored in Oracle tables which will be available via the NFIP IT Business Objects Reporting Tools.

- Computer Associates Identity Manager generates user and website access logs
- The NFIP Location Validation application generates audit logs to report statistics on the types of property addresses accessed within NFIP IT
- Oracle logs are generated to provide information on accessed table-spaces

3.13 Specific Equipment/Service Restrictions.

The use of specific prohibited or restricted services, protocols, and ports listed in the DHS 4300A System Security Handbook (SSH) require an approved waiver or exception agreement between the system DAAs. Any additional interconnections to NFIP IT Systems outside of the of WYO Company, Vendor and FEMA NFIP stakeholder community shall be documented in the appropriate security documentation and each party shall be notified of the new interconnections.

3.14 Remote Connectivity.

FEMA NFIP IT contractors currently use Juniper NetScreen Remote Admin Client for remote VPN access to the ***FEMA NFIP IT Systems***.

3.15 Training and Awareness

Both parties will ensure that all individuals using the systems (i.e., ***FEMA NFIP IT Systems*** and ***[WYO Company or Vendor System Name]***) have attended initial basic and annual refresher Computer Security Awareness and Training. Additionally, both parties will ensure that persons with significant security responsibilities for the systems receive annual role based training covering their specific areas of responsibility. This training should ensure that staff members know how to report suspicious or prohibited activities.

3.16 Security Documentation

The ***FEMA NFIP IT Systems*** and ***[WYO Company]*** Certification and Accreditation (C&A) ***or comparable*** documentation (e.g., System Security Plan, Contingency Plan, Risk Assessments

FOR OFFICIAL USE ONLY

and Security Assessments, Interconnection Security Agreements, etc.) and all other security related documents will be made available to each party for review and acceptance upon request. C&A documentation will be updated to reflect the establishment of this interconnection and whenever a significant system change occurs or at least annually. This MOU shall be updated should any of the information contained within change. The following information, at a minimum will be accurately maintained within this MOU:

- Names of WYO Companies or Vendors
- Organizations owning the other systems
- Type of Vendor Relationship
- Name and title of authorizing management officials (e.g. Chief Information Officer or Designated Authorizing Authority)
- Interaction among the WYO and NFIP IT Services
- Rules of Behavior

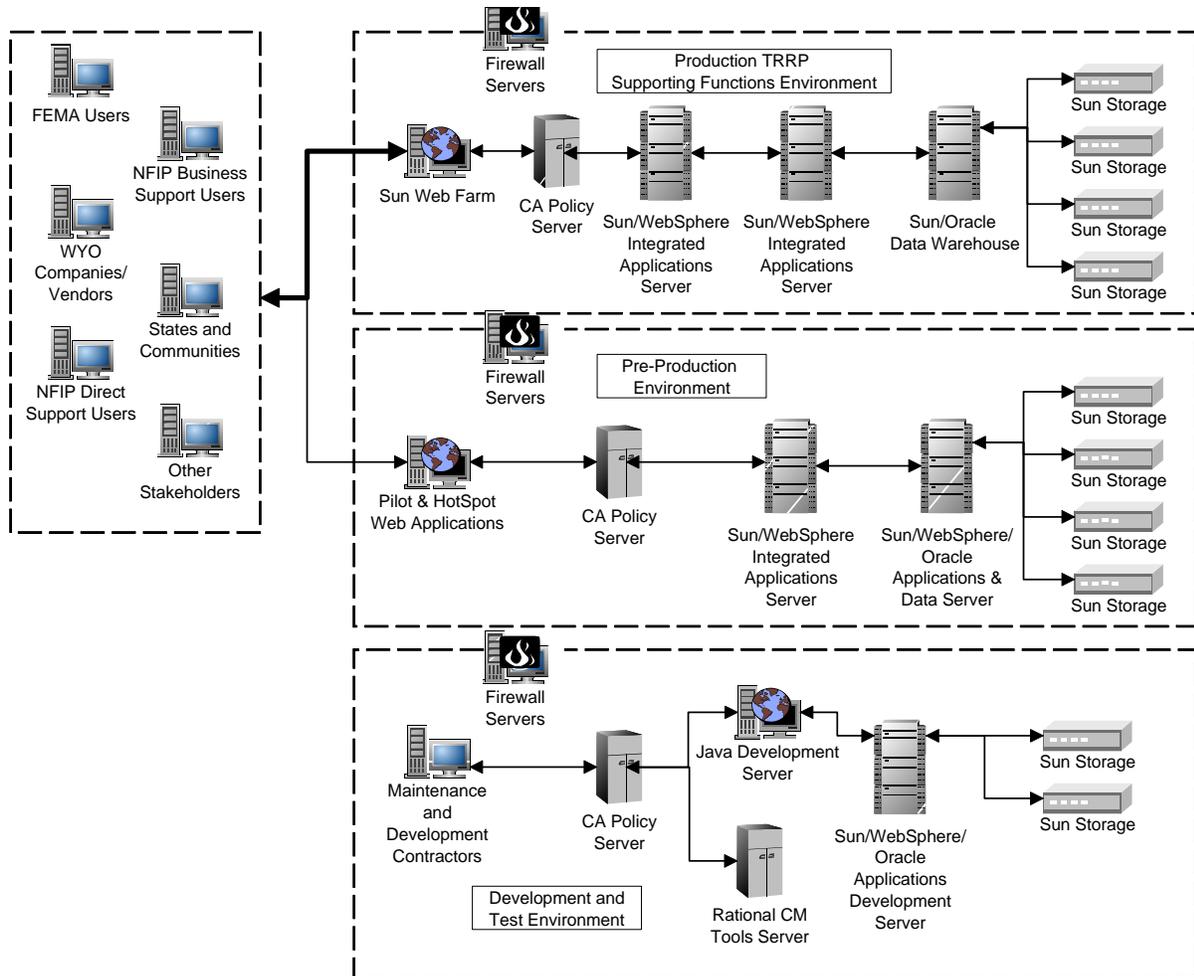
All future changes relating to the security architecture of either system will be updated within the corresponding security documents. The assigned Information System Security Officer(s) for each system shall provide the security documentation to the each organization upon request.

3.17 Change Control

Significant changes to the system architecture, documentation, or configurations will be reviewed, approved and documented in accordance with each organization's configuration/change control process. FEMA NFIP IT Systems fall under the Program Management Office of the Mitigation Directorate Insurance Operations Section. NFIP IT will utilize Capability Maturity Model Integrated Level 3 framework to govern its ongoing systems operations. Each organization shall notify the other if a system change significantly changes the approved security posture of the system or introduces new significant residual risk to either system. Whenever significant changes are made at one or both organizations, e.g., through additional staff , service, etc., this should be recorded as an addendum to the original MOU.

4.0 TOPOLOGICAL DRAWING

An architecture diagram showing the system interconnection is contained in Attachment A. The diagrams shall illustrate all communication paths, circuits, and other components used for the interconnection.



FOR OFFICIAL USE ONLY

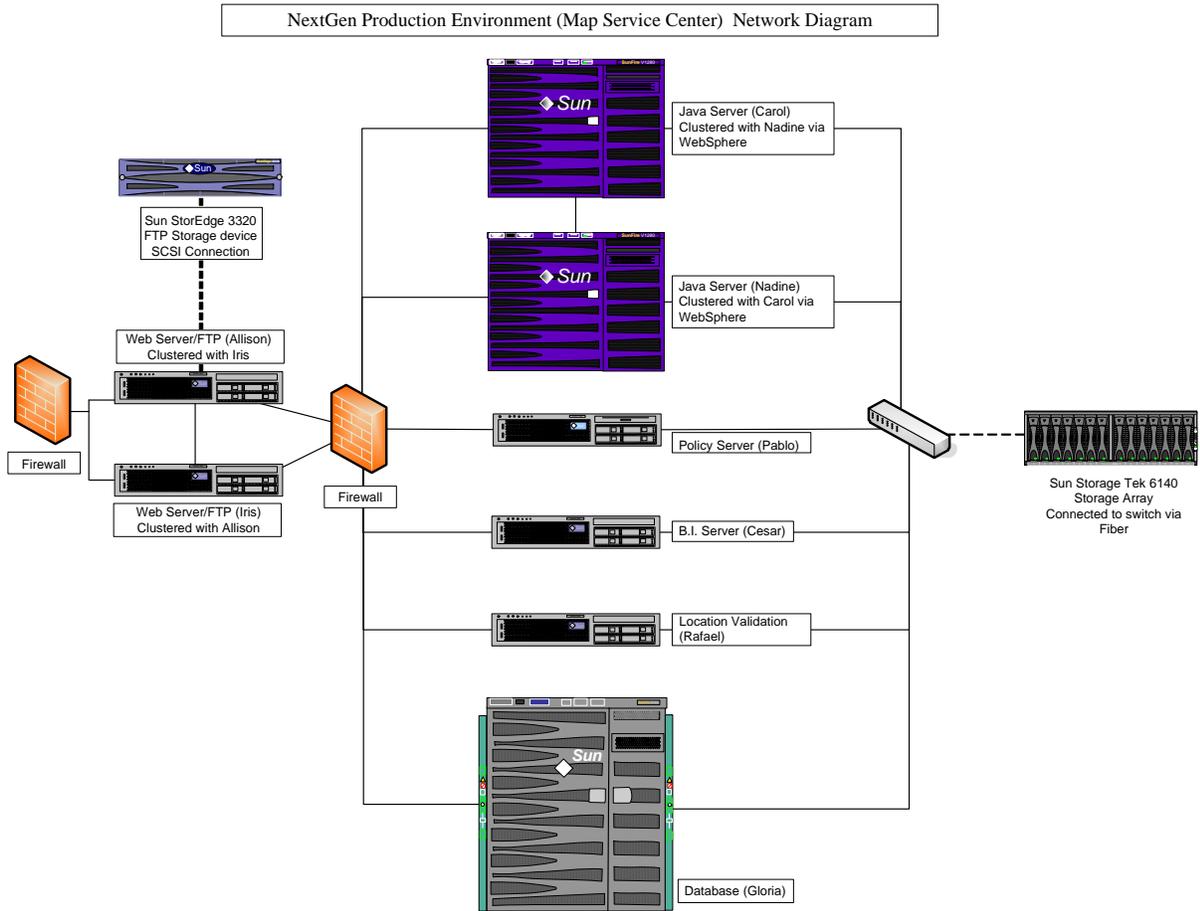
5.0 SIGNATORY AUTHORITY

This MOU is valid for three (3) years after the latest date on either signature listed below, if the technology documented herein does not change or if there are no other intervening requirements for updates. At that time it must be reviewed, updated, and reauthorized. The security controls for this interconnection will be reviewed at least annually or whenever a significant change occurs. Either party may terminate this agreement with thirty days advanced notice. Noncompliance on the part of either organization or its users or contractors with regards to security policies, standards, and procedures explained herein may result in the immediate termination of this agreement.

DHS FEMA Mitigation Directorate NFIP IT Systems Designated Accrediting Authority (DAA) David Maurstad or Ed Connor	
Signature & Date	
<i>[WYO Company or Vendor]</i> DAA Name	
Signature & Date	

Attachment A:

FEMA NFIP IT Systems (aka NextGen) Architecture Diagram is provided below. All WYO Companies and Vendors systems' will submit and retrieve batch data via the FTP resources identified below.



FOR OFFICIAL USE ONLY

Attachment B

DHS Incident Response Guidelines

Incidents must be prioritized and handled accordingly. As additional information becomes available, the priority and criticality of the incident may change. Common sense, knowing when to escalate an incident, and the ability to reprioritize are critical incident handling skills necessary for an incident handler at both Organizational Element and Department levels. The following table provides the initial response for each incident type required to be reported to the DHS SOC.

Incident Type	Criticality	Action
Unauthorized Access (Intrusion)	Significant - Unauthorized access with system-level or user-level privileges to critical or line-of-business systems/applications	Telephone notification to DHS SOC immediately after the Component SOC validates an actual or suspected incident. Follow-up reports every 24 hours until closed.
	Minor - Limited unauthorized access that does not jeopardize Component mission capability or provide possible access to critical systems	Weekly report to DHS SOC
Denial of Service (DoS)	Significant – Critical system or network resources are unavailable for use by the authorized user community due to attack activity (malicious or inadvertent)	Telephone notification to DHS SOC immediately after the Component SOC validates an actual or suspected incident. Follow-up reports every 24 hours until closed.
	Significant – General system or network resources are unavailable on a large scale (20 or more systems) for use by the authorized user community due to attack activity (malicious or inadvertent)	
	Minor - Small scale (19 or less users) system or network resources for general line-of-business applications/services are unavailable for use by the authorized user community due to attack activity (malicious or inadvertent), and attack source is known and no likelihood of further attack exists (internal incident)	Weekly report to DHS SOC

FOR OFFICIAL USE ONLY

Incident Type	Criticality	Action
Malicious logic (Virus, Trojan, Worm, etc.)	Significant – Critical systems are infected by malicious logic.	Telephone notification to DHS SOC immediately after the Component SOC validates an actual or suspected incident. Upon notification, an incident is opened and all infections of the same type are tracked under that incident number until all infections are eradicated. The Component SOC provides updates every 24 hours on the number of infections involved with the incident and status of eradication efforts. After incident is closed, if additional infections are discovered, a new incident is opened.
	Significant – Widespread (10+) infections by malicious logic affecting line of business systems.	
	Significant – Malicious logic is discovered that is not detected by system protective measures (virus protection, etc.)	
	Minor - Any malicious logic infection not listed as significant above.	Weekly report to DHS SOC
	Minor - Any malicious logic stopped by system protective measures at DHS external email gateways and/or relays. (Malicious logic stopped by system protective measures on other devices such as workstations and servers will not be reported as incidents)	Tracked daily by DHS SOC
Misuse	Significant - An authorized user violates Federal law regarding proper use of computer resources.	Telephone notification to DHS SOC immediately after the Component SOC validates an actual or suspected incident. Follow-up reports every 24 hours until closed.
	Minor - An authorized user commits a serious violation (as defined by the Component) of Departmental or Component computer security policies May include use of unauthorized: <ul style="list-style-type: none"> • chat programs • peer to peer services • password/account sharing • personal use of government resources or information • remote control software • insecure services/protocols • etc. 	Weekly report to DHS SOC

FOR OFFICIAL USE ONLY

Incident Type	Criticality	Action
<p>Probes and Reconnaissance Scans (Internal to DHS network only. Does not include probes and reconnaissance scans taking place on internet facing connections)</p>	<p>Significant – Unusual or threatening unauthorized system probing and/or data gathering directed specifically toward critical systems</p>	<p>Telephone notification to DHS SOC immediately after the Component SOC validates an actual or suspected incident. Upon notification, an incident is opened and remains open until the specific probing activity ends. The Component SOC updates DHS SOC every 24 hours on the numbers and types of probes associated with the probes and reconnaissance scans until the incident is closed.</p>
	<p>Significant - Unauthorized System probing and/or data gathering originating from entities known or suspected to be a threat to national security</p>	
	<p>Significant - Unauthorized System probing and/or data gathering that appears to be widespread and/or unusually threatening</p>	
	<p>Significant - Unauthorized system probing that penetrates network perimeter defenses with the capability of gathering information from internal resources</p>	
<p>Classified Computer Security Incident</p>	<p>Significant – Classified information is introduced to a computer system/device that does not have the appropriate classification level or is transmitted without appropriate protection.</p>	<p>Telephone notification to DHS SOC immediately after the Component SOC validates an actual or suspected incident.</p> <p>The DHS SOC will proceed to immediately notify the Director of IT Security Operations or the CISO in his absence. In turn, the Director of IT Security Operations or the CISO will notify the CSO as follows: Notify Director of Classifications Division for any classified incident and Director of Special Security Programs Divisions for any SCI or intelligence related event. Criminal activity is reported to the Investigations Division.</p> <p>Follow-up reports every 24 hours until closed.</p>
	<p>Significant - Any security incident that involves a system used to process national security information</p>	
<p>Alteration/Compromise of Information</p>	<p>Significant - Any incident that involves the unauthorized altering of critical information, or any incident that involves the compromise of critical information</p>	<p>Telephone notification to DHS SOC immediately after the Component SOC validates an actual or suspected incident. Follow-up reports every 24 hours until closed.</p>
	<p>Minor - Any incident that involves the unauthorized altering of sensitive information, or any incident that involves the compromise of sensitive information that does not seriously jeopardize DHS/Component mission</p>	<p>Weekly report to DHS SOC</p>

FOR OFFICIAL USE ONLY

Incident Type	Criticality	Action
Multiple Component	Significant - Any incident involving events considered significant incidents in more than one of the above categories	Telephone notification to DHS SOC immediately after the Component SOC validates an actual or suspected incident. Follow-up reports every 24 hours until closed.
	Minor - Any incident involving events considered minor incidents in more than one of the above categories	Weekly report to DHS SOC