Defense Security Service

National Industrial Security Program Authorization Office

National Industrial Security Program Enterprise Wide Area Network (NISP eWAN) System Job Aid

This page intentionally left blank.

EXECUTIVE SUMMARY

The policy of the U.S. Government is that all classified information must be appropriately safeguarded to assure the confidentiality of that information, as well as the integrity and availability of that information when required by contract. This Defense Security Service (DSS) National Industrial Security Program (NISP) Enterprise Wide Area Network (eWAN) System Analysis Process is intended for use by participating Cleared Industry Contractors. The content provides a description of the overarching eWAN policies that support eWAN request submissions for DSS review and assessment activities that lead to an authorization decision.

Record of Changes

This document is managed by the NISP Authorization Office and the eWAN Program Manager. Major revisions are indicated by the number to the left of the decimal point while minor revisions are indicated by the number to the right. Major revisions occur when major policy or process changes render the prior version obsolete or there are more than 10 minor changes. The table below is updated upon change and version approval. The release date reflects when the content was approved for external use.

Version	Content or Change	Approver	Release Date
1.0	Initial Internal Release	K. Hellmann, NAO J. Cofer, NISP eWAN PM	5 April 2019
1.1	Initial External Release, URLs and Terms Updated	J. Cofer, NISP eWAN PM	15 April 2019

Table of Contents

This page intentionally left blank.

1.0 eWAN Concept

Introduction

The National Industrial Security Program Enterprise Wide Area Network (NISP eWAN) concept allows NISP participants to design and develop an enterprise WANs (eWAN) to operate and maintain NISP systems under a single Authorization to Operate (ATO). Cleared Industry companies seeking to design and develop a NISP eWAN must meet certain criteria to own and operate a eWAN. Once eligibility has been determined, the company must provide a NISP eWAN Proposal to the NISP Authorization Office, Defense Security Service.

NISP eWAN Operational Criteria

For a Cleared Industry participant to establish an eWAN, the organization must meet the following criteria:

- Currently operating at least one NISP system located in two or more DSS geographic regions
- Have program/contractual requirements appropriate for an eWAN
- Have or plan to implement a centralized network operations/security operations centers facilitating centralized management and threat monitoring of multiple geographic locations
- Development of a single comprehensive enterprise network topology design
- Develop and implement centralized administrative policies and procedures governing operation and monitoring of the eWAN topology
- Designate an information system security manager (ISSM) of record for the NISP eWAN.

Each NISP eWAN will be unique to the Cleared Industry business objectives, risk tolerance, and security posture required to support the system operations. These concepts will be integrated into the proposal provided to the NISP Authorization Office for analysis and eWAN concept approval.

System Objectives

The eWAN Process core objectives are to:

- Provide standardized system management and support services
- Enhance security posture via an enterprise Authorization to Operate (ATO)
- Standardize continuous monitoring and reporting
- Leverage common controls from the eWAN to supported subsystems
- Reduce Cleared Industry administrative burden by reducing the number of ATOs requiring management

Each organization must assess system objectives based on the corporate business model, capabilities, and strategies specific to the participant's unique operations.

eWAN Concept, *Continued*

1.1. Enterprise Wide Area Network Concept Development

Concept Core Model

The NISP eWAN concept model links enterprise business strategy and IT operations to the NISP systems in operation across the organization. The eWAN capability operates as a strategic asset at the corporate level in support of classified programs.

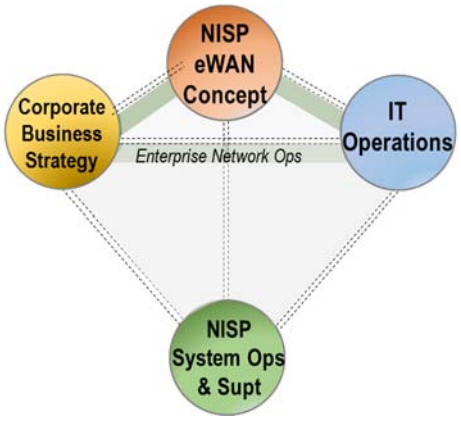

Figure 1.1 NISP eWAN Concept Model

Each Cleared Industry participant has a unique enterprise IT model mapped to specific program requirements and IT capabilities. The concept model in Figure 1.1 provides a simple relational model, but the corporate model could be much more complex based on number of systems, security requirements, and operational requirements.

Concept Purpose

The NISP eWAN concept allows cleared industry participants who meet specific criteria to consolidate classified program work and security operations corporate-wide securely within a single Authorization to Operate (ATO). Figure 1.2 captures the NISP systems transition to a single Authorization to Operation for a consolidated NISP eWAN.

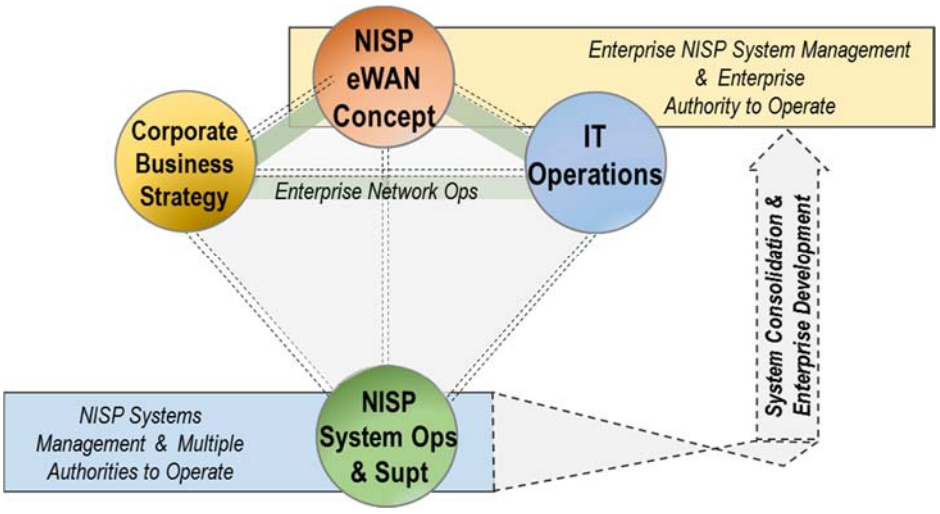

Figure 1.2 NISP Enterprise Wide Area Network Operational Transition Concept

1.2. eWAN Initiation and Requirements

Overview

The prospective eWAN participant must establish a point of contact (POC) within the contractor organization to interface with DSS NAO. This POC should have the ability to commit resources and personnel to the design, implementation, assessment, and operation of the proposed corporate classified network.

The eWAN POC will lead the industry team through the process. See Figure 1.3 for an overview of a generic eWAN development process from Industry's perspective.

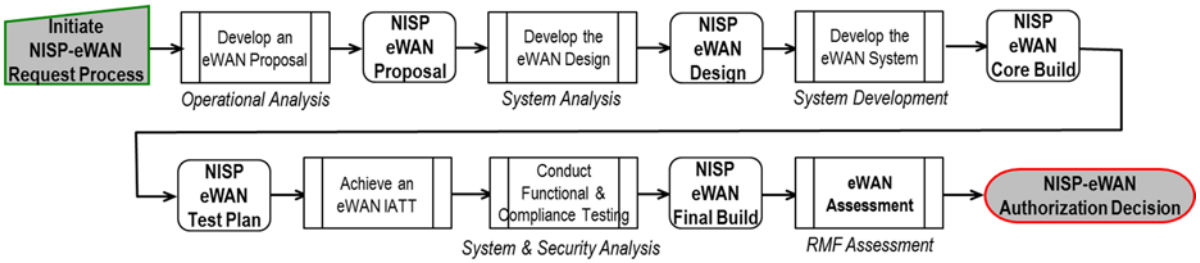

Figure 1.3 NISP Enterprise Wide Area Network Process Overview
(Process Projection)

System Objectives

The eWAN Process achieves the following system objectives:

- Provides standardized system management and support services
- Enhances security posture via an enterprise Authorization to Operate (ATO)
- Standardizes continuous monitoring and reporting
- Leverages common controls from the eWAN to connected subsystems
- Reduces administrative burden by reducing the number of ATOs requiring management.

Each organization will assess system objectives based on corporate business models and strategies specific to their operations.

eWAN Requirements

NISP participants pursuing an eWAN must determine the program and operational requirements to develop and operate a NISP eWAN are present. This job aid will identify three types of requirements as follows:

- Organizational Requirements
- Operational Requirements
- NISP eWAN System Requirements

eWAN Concept, *Continued*

1.2.1. Organizational Requirements

eWAN Training Requirements

Organizations requesting a NISP eWAN may be required to meet additional training requirements as determined by DSS NAO. The Industry eWAN PM will ensure that all required training is completed by eWAN System Administrators. Below are examples of training that may be required:

DISA Information Assurance Support Environment (IASE) Training

Available at: (https://iase.disa.mil/Pages/index.aspx)

- Cyber Awareness Challenge
- Enterprise Mission Assurance Support Service (eMASS) Training * – *View All* Role

* NOTE: Common Access Card or ECA required to access and complete training

DSS Center for Development of Security Excellence (CDSE)

Available at: (https://www.cdse.edu/)

- Risk Management Framework (RMF) training

Organizations may define additional training requirements for eWAN teams based on program or operational requirements.

1.2.2. Operational Requirements

Enterprise Management & Control

The NISP eWAN capability will require Cleared Industry participants to:

- Assign a Corporate ISSM/POC for the eWAN
- Obtain a NISP-eMASS Corporate Container for eWAN RMF support
- Establish eMASS accounts for appropriate personnel
- Develop enterprise continuous monitoring strategies and implementation methodologies.
- Establish centralized management, user administration, vulnerability management, change management, and configuration management controls.

These capabilities are required as part of the eWAN proposal and eventual operational build of the NISP eWAN. Many companies may have existing enterprise infrastructure to support corporate IT operations. The NISP eWAN may leverage much of the transport capabilities to interconnect and interoperate the NISP eWAN, but a secure network must be designed and operated on its own architecture.

eWAN Concept, *Continued*

1.2.3. NISP Enterprise Requirements

eWAN Controls

The NISP eWAN must address every security control at the level commensurate with the Risk Assessment of the proposed e-WAN. When categorizing the eWAN consideration should be given to the sensitivity of the programs the network will support.

The requirement is to address all security controls in the DSS Moderate-Low-Low baseline at a minimum, independent of the system type or overlay. This approach provides Cleared Industry the opportunity to integrate additional NISP systems to the NISP eWAN as required.

NISP-eMASS Support

The DAAPM overlays are integrated into the NISP-eMASS instance and are available to support the NISP systems. The following apply to eWANs:

- NISP eWANs will not have an overlay
- Every control must be addressed as part of the enterprise operational methodology
- All risks to be appropriately mitigated
- The eWAN must not be registered as a new system in the NISP eMASS until the eWAN proposal has been reviewed and approved by NAO

The NISP-eMASS processes and procedures will apply equally to the NISP eWANs to complete the eMASS content, so the appropriate corporate IT and Security staff will require a NISP-eMASS account as assigned. The Cleared Industry eMASS accounts will be assigned to the Control Approval Chain Role 1.

1.3. References

Overview

The following reference will assist the Cleared Industry teams assigned to NISP eWAN opportunities. See Table 1.2 for the references supporting the security analysis and control implementation for the eWAN. Additional information is listed in Table 1.3 to assist the eWAN development team.

When the following standards are superseded by an approved revision, the revision shall apply.

Table 1.2 eWAN Security References & Support

Short Title	Reference Name
CNSS Inst No. 1253	*Security Categorization and Control Selection for National Security*
CNSSD 504	*Directive on Protecting National Security Systems from Insider Threat*
CNSSP 11	*Acquisition of Information Assurance (IA) and IA Enabled Information Technology (IT) Products, Dated 01 2013 [Supersedes NSTISSP-11]*
DAAPM v2.x	*Defense Security Service (DSS) Assessment and Authorization Process Manual (DAAPM)*
DoDM 5220.22-M w/Ch2	*National Industrial Security Program Operating Manual (NISPOM) dtd May 18, 2016*
NIST SP 800-37, Rev 3	*Guide for Applying the Risk Management Framework (RMF) to Federal Information Systems*
NIST SP 800-53 Version (4)	*Recommended Security and Privacy Controls for Federal Information Systems and Organizations*
NIST SP 800-53A, Rev 4	*Guide for Assessing the Security Controls in Federal Information Systems and Organizations*
NIST SP 800-115	*Technical Guide to Information Security Testing and Assessment*

Table 1.3 eWAN Support References

Reference Resource	Website Location
DSS Risk Management Framework Information & Resources	*https://www.dss.mil/ma/ctp/io/nao/rmf/*
Committee on National Security Systems (CNSS)	*https://www.cnss.gov/CNSS/*
National Information Assurance Partnership (NIAP)	*https://www.niap-ccevs.org/ccevs/defined/*
National Institute of Standards and Technology (NIST) Computer Resource Center	*https://csrc.nist.gov/Publications/*

2.0 Developing the NISP eWAN Proposal

Overview

The NISP eWAN proposal is developed by Cleared Industry to provide the NISP Authorization Official with a strategic view of how the NISP systems will interoperate as an enterprise system within the Enterprise Wide Area Network (eWAN) construct. Figure 2.1 provides a projection of a generic process that may be similar to methods Cleared Industry would use to develop a system proposal.

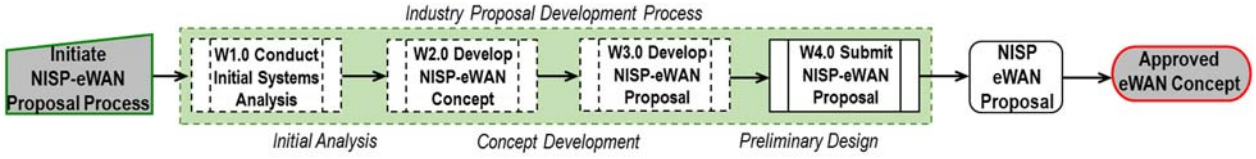

Figure 2.1 NISP eWAN Proposal Process
(Process Projection)

2.1. Proposal Support Concepts

Overview

The NISP eWAN proposal requires the developer to understand how the organization will define the system concept within risk and operational parameters as defined by their organization. This subsection addresses the overarching concepts that may impact the eWAN proposal development.

While every NISP eWAN will be designed and developed based on individual Cleared Industry business strategies and objectives, many organizations may not have enterprise planners or staff experts. This information is provided as potential definitions of the core information contained in an eWAN proposal.

Proposal Core Elements

The core elements that may assist in the eWAN proposal development team are as follows:

- Corporate Governance
- Deployment of Network/Security Operation Centers
- Interconnected Node Sites
- Integrated or Supported NISP Systems
- Supported Programs
- eWAN Concept
    - o System Concept
    - o Security Concept
    - o Enterprise Operational Concept

Additional information may be required based on system complexity and the operational concept the system supports. .

Proposal Support Concepts, *Continued*

Corporate Governance Model

The corporate security governance within the NISP eWAN provides active management at the corporate suite level or equivalent for coordination, development, and operation of the eWAN. An active corporate governance model for the eWAN may be implemented by individuals or groups within the organization with the authority to pursue a corporate-scale endeavor.

Enterprise WAN Architecture

The NISP enterprise-level topology describing how component NISP systems are interconnected, allowing centrally administered security operations and real time monitoring; system and security capability consolidation within a centralized management plan.

Node	A node is a point of intersection/connection within a network. In an environment where all devices are accessible through the network, devices located within the same geographical location (as defined by CAGE code) behind the encryption device will be considered "nodes".

Interconnected (Network) **Node System**	A system of physically or logically separated systems administered under common security, access management, and operational requirements. The boundary of an individual constituent node is defined by the system/network architecture downstream of the encryption device. However, all participant nodes are centrally managed via shared policies and procedures.

Enterprise WAN Management

The NISP eWAN provides enterprise-level IT capabilities and services to include maintaining situational awareness of all network operations and security of the NISP eWAN infrastructure, computing, and enterprise services. The core elements or capabilities within the eWAN construct are the:

- Network Operations Center (NOC)
- Security Operations Center (SOC)

The functions within the NOC/SOC environments should be designed to support the interconnected NISP systems as part of the LAN/WAN design. Each NOC/SOC capability will be based on the NISP systems security plan and functional requirements.

Proposal Support Concepts, *Continued*

Network Operations Center (NOC)	A network operations center (NOC) is a place from which administrators supervise, monitor and maintain a telecommunications network. Large enterprises with large networks as well as large network service providers typically have a network operations center, a room containing visualizations of the network or networks that are being monitored, workstations at which the detailed status of the network can be seen, and the necessary software to manage the networks. The network operations center is the focal point for network troubleshooting, software distribution and updating, router and domain name management, performance monitoring, and coordination with affiliated networks.

Security Operations Center (SOC)	A security operations center (SOC) is a facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis. The SOC team's goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes. Security operations centers are typically staffed with security analysts and engineers as well as managers who oversee security operations.

Enterprise Concept of Operations (CONOPS)

The eWAN CONOPS presents a strategic overview of how the participants will connect, secure, and operate the proposed NISP eWAN. Each eWAN proposal will be unique to the participant and the preliminary concept could be based on the following parameters:

- Business Objectives
- Customer Program Support
- Common Operational Requirements
- Personnel Distribution and Expertise
- Enterprise Common Controls
- Technological Capabilities

NOTE	These content elements are suggested to assist; not to direct or limit the Cleared Industry participants during the eWAN proposal development. Each NISP participant must tailor a plan for their organization.

Proposal Support Concepts, *Continued*

Business Objectives	Cleared industry must conduct an analysis of currently supported programs, customer expectations, return on investment, and opportunities for growth, efficiency improvements, and administrative requirements to determine if the NISP eWAN is an appropriate solution.

Customer Program Support	The customer is the information owner for classified data, and contractual obligations/restrictions must be considered before leveraging shared information technology resources in an enterprise classified network. Security Classification Guides (SCGs), contract language, and individual constituent program requirements must be taken into account when engineering a corporate-wide classified network solution.

Common Operational Requirements	Deployment of an enterprise classified network within the NISP requires careful analysis of the operational requirements of the programs intended for inclusion; ensuring that overarching administrative and security policy can be written or leveraged across the enterprise as high in the architecture as possible.

Personnel Distribution and Expertise	The NISP eWAN allows an organization to centralize security and administrative operations, allowing ISSMs/ISSOs to manage the network from operations centers distributed throughout the network. This capability can be leveraged to share the knowledge and subject matter expertise of IA experts regardless of the physical facility location.

Enterprise Common Controls	Corporate policies and procedures can be written or modified to apply to all constituent systems within the eWAN boundary. This allows for the leveraging of common control packages that address multiple security control families across all members of the enterprise.

Technological Capabilities	Successful deployment of the NISP eWAN allows for leveraging of innovative technological solutions such as Commercial Solutions for Classified (CSfC), Virtualization, real-time vulnerability assessment, and automated patching. Organizations should explore appropriate solutions that match program requirements with possible increases in administrative and operational efficiency.

Proposal Support Concepts, *Continued*

Using the eWAN Concepts and Terms

The terms and definitions presented in this document are provided to core system elements and activities contained in an eWAN at the conceptual level. The NISP participants will leverage individual operational and technical processes, procedures, and technical terminology proprietary to their operations.

NISP participants seeking to leverage the eWAN solution will be required to execute the following major steps:

- Develop an Operational Concept to support the eWAN Proposal
- Develop an eWAN Design
- Construct a System Security Plan, Test Plan, and Evaluation Schedule in coordination with DSS NAO within the NISP eMASS instance
- Prepare for DSS NAO Validation and Authorization

2.2. Conducting the Initial Analysis

Overview

Each company will use their proprietary proposal development process, system development process, or a hybrid of the two to support the NISP eWAN proposal development. Figure 2.2 provides a generic process projection of the suggested work to develop a NISP eWAN proposal. This process projection step will have supporting content introduced within each subsection.

NOTE	**The system is not to be registered in the NISP eMASS instance until the eWAN proposal has been approved by NAO.**

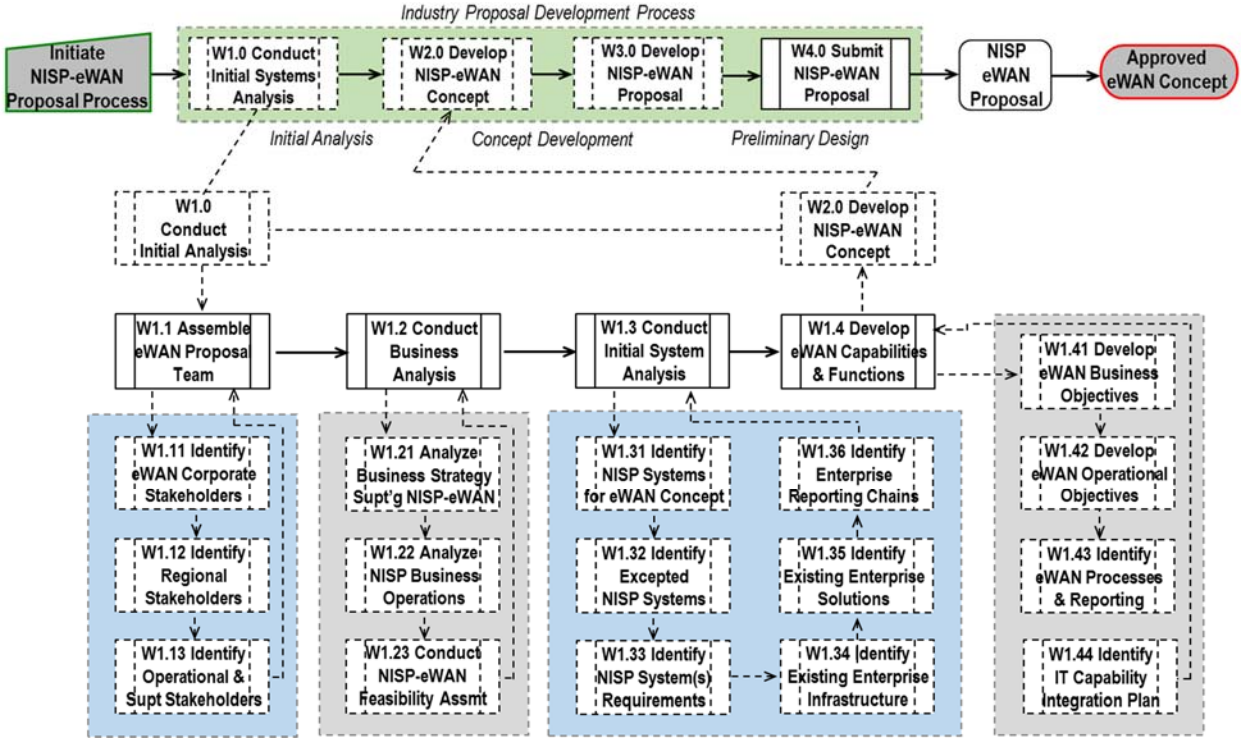

Figure 2.2 eWAN Proposal Development Process
(Process Projection)

Preliminary eWAN Analysis

The NISP participant should conduct a preliminary assessment of the NISP eWAN concept at the corporate level. Some of the considerations may include:

- Analysis of the system operating environment
- Development the initial Operational Concept or Conceptual Design
- Assessment of the Operational Concept against the Business Strategies
- Analysis of the quantitative and qualitative benefits of integrating the NISP systems into a single architecture under one authorization

Conducting the Initial Analysis, *Continued*

Initiating the Proposal Tasks

Once the Cleared Industry company has made the preliminary decision to move forward on a NISP eWAN, the next step is to assign the NISP eWAN initiative point of contact and determine who should participate on the eWAN proposal. This document assumes that an eWAN team will be assigned, but each company will have to make that determination based on the project complexity and the concept of operations.

2.2.1. Assembling the eWAN Team

Introduction

The NISP eWAN team reflects the eWAN approach that the company selects to pursue based on the corporate model and desired NISP eWAN capabilities required to operate the network. Compounding factors in determining the group structure are factors such as complexity, geographic dispersion, and management tasks required to operate and maintain the eWAN.

NISP eWAN ISSM of Record

Each NISP eWAN requires a corporate point of contact and ISSM of Record to operate and monitor the system. Organizations must identify a specific individual to be the ISSM of Record, which may or may not be delegated based on the business operations model. This responsibility could be assigned to a role such as:

- Chief Information Officer
- Chief Risk Officer
- Corporate Information Systems Security Officer
- Corporate Director of Cybersecurity
- Other assigned responsible party

Enterprise Stakeholders

To ensure support at the organizational level, the eWAN team should identify the following:

- Identify Corporate Stakeholders
- Identify Regional Stakeholders
- Identify Operational & System Stakeholders
- Identify Customer Program Stakeholders

Conducting the Initial Analysis, *Continued*

2.2.2. Conduct the Initial System Analysis

Overview

The Initial System Analysis will be unique to each Cleared Industry, so the preliminary tasks may need to start at the business enterprise network level. The initial questions could be similar to the following:

- Evaluate the NISP systems in the "corporate" portfolio or "business unit" portfolios
- Determine if a corporate enterprise exists
- Determine if the corporate enterprise architecture could support a NISP eWAN deployment and operation
- Analyze the corporate enterprise network for supporting capabilities
- Analyze any corporate enterprise systems, services, and processes for applicability and deployment within a secure operating environment

Each NISP participant will have to develop their own initial analysis based on their business strategy, existing architecture, and adaptability of their current operations to expand and/or operate a secure environment for a NISP eWAN.

Initial Analysis Model

The following strategic tasks could form an initial analysis model:

- Evaluate current NISP systems
- Evaluate the corporate/company IT infrastructure
- Evaluate Enterprise architecture if one exists
- Evaluate the Enterprise or Potential Enterprise Solutions

Each company may have to create a unique model to support their business and mission objectives.

NISP System Analysis

This task will be unique to each company if this task applies. The approach may be simple or complex based on the number of systems, dispersion, configuration, potential for interoperation, and enterprise supportability. The core analysis may focus on similar objectives as follow:

- Identify NISP systems and system locations
- Identify NISP systems with potential for eWAN inclusion
- Identify NISP systems with multiple site deployments
- Identify NISP systems with like configurations
- Identify NISP systems *ineligible for incorporation* into the eWAN due to customer, program, or contractual restrictions

Conducting the Initial Analysis, *Continued*

Corporate IT Infrastructure Analysis

Evaluating the corporate IT infrastructure for NISP eWAN supportability is a preliminary step to identify existing IT infrastructure and solutions that could be leveraged. Convergence of business unit IT infrastructures into a corporate eWAN may be the scope of the initial NISP eWAN analysis.

Enterprise	An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. *[CNSSI 4009, p. 49.]*

Enterprise IT	Enterprise IT consists of enterprise architecture; technical evolution; preliminary design of data centers or infrastructure components; implementation, monitoring, and operations of infrastructure; and technical governance. Critical areas of focus normally include: information assurance, data strategy, interoperability, application integration, information exchange, networks, and communications services (voice, video, and data).

Enterprise Risk Management	The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of: • Enterprise capabilities • Mission dependencies on enterprise capabilities • Risks and prioritization due to defined threats • Countermeasure implementation to provide both a static risk posture and an effective dynamic response to active threats • Enterprise performance assessment against threats • Countermeasure adjustments as necessary to reduce/eliminate risk *[CNSSI 4009, p. 49.]*

NISP Enterprise Wide Area Network (NISP eWAN)	A NISP enterprise WAN (eWAN) is a corporate classified network that connects geographically dispersed systems and subnetworks at cleared contractor facilities around the country. As is the case with most WANs, a NISP enterprise WAN links authorized WANs and LANs in multiple locations.

Conducting the Initial Analysis, *Continued*

Enterprise Solution Analysis

Facilities should analyze existing authorized networks as well as corporate enterprise IT capabilities to determine how to merge these resources to facilitate a corporate classified network solution.

A potential approach may be to:

- Identify Enterprise systems and supporting capability requirements
- Identify the organizational structure and operational support requirements
- Consider the operational and security control hierarchy if one exists
  - *If no control hierarchy exists*, the gap may become part of the eWAN design
- Identifying operational and maintenance support systems to support
  - Monitoring
  - Reporting
  - Security
  - Process management such as: Change Management, Configuration Management, Access Management, and other processes

Every company will have a unique analysis to support a NISP eWAN decision.

2.3. Developing the System Concept

Introduction

Once the Cleared Industry participant has made the determination that a NISP eWAN is an appropriate and feasible solution, the company will designate a responsible party to serve as the primary point of contact for coordination with DSS NAO. Figure 2.3 contains a system concept map.

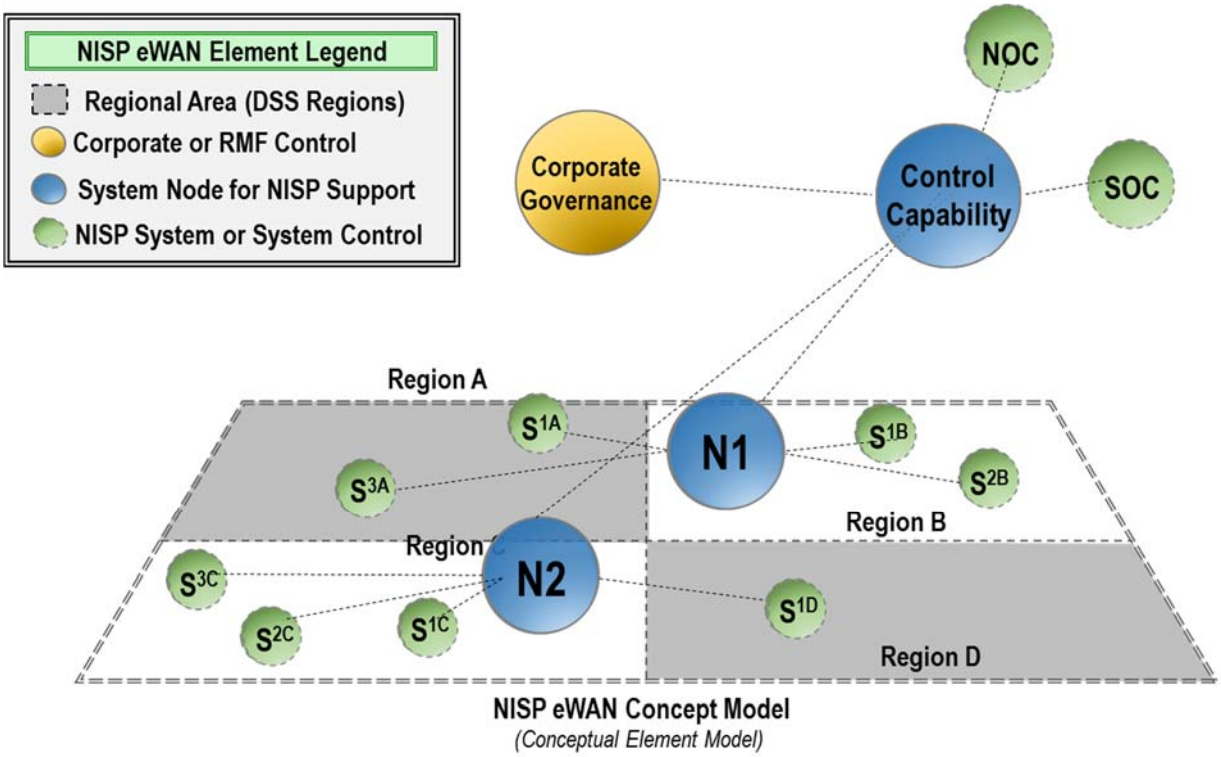

Figure 2.3 NISP eWAN Concept Model with Conceptual Elements

Confirm eWAN Criteria

The NISP eWAN must meet the following criteria:

- The eWAN authority and oversight resides at the Corporate level
- The proposed enterprise WAN is centrally managed, operated, and secured via use of security and/or network operations centers
- Network nodes located in at least two DSS regions
- Network NOC/SOC provides enterprise network operational and security services to the connected NISP systems
- Transport between nodes and the NOC/SOC are secured by end-to-end encryption/secure tunneling and protected distribution systems (PDS where applicable).

Conducting the Initial Analysis, *Continued*

eWAN Front End Analysis

Each company will conduct the business analysis or front end analysis on the NISP systems to ensure that an eWAN proposal meets the criteria and serves the corporate business strategy.

In addition to the eWAN criteria, the eWAN proposal lead may have to conduct the initial analysis to verify eWAN criteria or objectives. Example questions may be similar to:

- How can current enterprise IT capabilities be leveraged to facilitate the NISP eWAN?
  (Existing Corporate WAN or infrastructure development?)
- What are the benefits of creating this capability?
  (Operating & Maintenance Costs, reduced risk, etc.)
- Will government customers require special configurations within the WAN to house and process their information?
  (Review programs, contracts, and applicable SCGs)
- Who are the expected end users?
  (System users, operator, administrators, and/or maintainers)
- Describe in detail functional requirements, preliminary (but quantitative) specifications, related technology areas, competitive benchmarks, and any related patents
- Comment on the scope of effort involved in general terms

2.3.1. Developing the Concept

Overview

The NISP eWAN will require the Industry eWAN team to categorize the results from the initial analysis into business, operational, and functional requirements. These requirements will be specific to the organization's business operations, technologies, integrated operational processes, and/or systems management. The NISP eWAN will have additional security requirements to enable security operations and support of classified systems.

Development Considerations

Identifying the development considerations to map the requirements against is the first step. Some possible considerations may be:

- Corporate Governance
- Network Infrastructure
- Node Integration
- Control Network
- Network Control
- Network Management
- Existing enterprise processes
- Existing enterprise capabilities
- Other Industry specific requirements

Developing the Concept, *Continued*

Corporate Governance

Coordination with DSS NAO requires designation of a corporate ISSM of Record for system operations and control. While this may be a strictly administrative control task at the corporate level, the designation becomes the point of contact for business operations and system control. The term could be interpreted to identify individuals at the corporate suite level who require situational awareness, visibility, or reporting if those system capabilities are mapped to an administrative control role versus an operational control role.

Network Infrastructure

A network infrastructure is the topology in which the *nodes* of a local area network (LAN) or a wide area network (WAN) are connected to each other. These connections involve equipment like routers, switches, bridges and hubs.

If an existing *enterprise architecture* exists, it may provide transport for the NISP eWAN and enterprise resources to enable a NISP eWAN solution. The corporate stakeholders such as the CIO, Chief Security Officer, Chief Risk Officer, and/or others as designated become players in the NIST eWAN concept development.

Enterprise Modelling	Enterprise modelling is the abstract representation, description and definition of the structure, processes, information and resources of an identifiable business, government body, or other large organization. Understanding an organization and improving its performance through creation and analysis of enterprise models to include the modelling of the following: • Relevant business domain (usually relatively stable) • Business processes (usually more volatile) • Uses of information technology within the business domain and its processes. Modelling supports enterprise architectures and network analysis.

Node Integration

Within the NISP eWAN program, a node is defined as a discrete segment of the network, located downstream of the end-to-end encryption device. Multiple "nodes" can exist within the physical boundaries of a facility provided each node is behind a separate encryptor. However it is uncommon in all but the largest facilities to have multiple nodes on an enterprise WAN within the confines of one facility/CAGE code.

Developing the Concept, *Continued*

Control Network

A Control Network is a network of nodes that collectively monitor, sense, and control or enable control of an environment for a particular purpose. These networks vary enormously in the number of nodes (from three to thousands) in the network and in complexity. Unlike networks that people use to communicate with each other, control networks tend to be invisible.

Network Control (Center)

Network Control (Center) is a single point of control with various network monitoring tools. This capability could be as small as a single software application up to a 'war room' with various monitoring tools in a large enterprise, Internet service provider, or communications carrier. Single point of control does not require co-location of capabilities nor integration with non-NISP capabilities unless so defined by the company defining the eWAN concept.

Within the NISP eWAN context, this could be the network operations and/or security operations capability used to operate and manage the NISP eWAN.

Enterprise Network Management

Enterprise Network Management an application or set of applications that lets network engineers manage a network's independent components inside a bigger network management framework performing several key functions. The NISP eWAN may be able to leverage existing network solutions to support some or all of the following:

- Network Operations
- Systems Operations
- Security Operations
- Network Monitoring
- Network Maintenance
- Network Reporting
- Others as applicable

The enterprise network management concept will assist the analysis by identifying scalable solutions, processes, and capabilities to support the NISP eWAN operations.

Enterprise Processes

The enterprise processes orchestrate organizational activities so that customers and their business achieve benefits. The advantages of identifying and managing the processes of an organization are the measurement, management and improvement systems and systems support. Enterprises with operational processes that are executed, aligned, and integrated is enhanced performance at reduced costs. Mapping the processes creates the functional requirements and supports the system and security interfaces.

Developing the Concept, *Continued*

Enterprise Process Maps	An enterprise process map: • Starts with the customer and identifies moments when the organization and the customer interact on a regular basis • Provides an end-to-end view of the processes spanning an enterprise to include business partners as part of the process mapping possibilities • Identifies how work flows through these processes to the end delivery of a solution for a customer • Identifies process intersections of supporting tasks, data, systems, and supporting management functions

Enterprise Capabilities

Enterprise capabilities are standard capabilities interconnected with and interdependent on business capability, process capability, information capability, IT capability, system offering and service offering. These influence strategic decisions and system development.

Industry Specific Requirements

Each Industry participant will have specific business and operational requirements that will be considered during the NISP eWAN analysis and development planning.

Development Outputs

The eWAN development process will be specific to the cleared contractor requesting a NISP eWAN. The development process will be specific to their needs, but this development process should provide the requesting cleared contractor with:

- eWAN Concept to enable the System Concept of Operations
- A preliminary NISP eWAN design
- An operational and support model(s) as required
- Rough order of magnitude for development if one is required

These elements would assist the eWAN team in developing the process with other Industry specific stakeholders.

2.4. Writing the Proposal

Introduction

The NISP eWAN proposal should provide the NISP Authorization Office with an operational view of how the company proposes the construction, operation, and monitoring of the eWAN. Each eWAN proposal will be unique to the company submitting the proposal based on the initial analysis.

NOTE	**The contractor organization shall not register the proposed eWAN system in the NISP eMASS instance until the eWAN proposal has been reviewed and approved by NAO.**

2.4.1. System Description or Situation

Introduction

The NISP eWAN proposal must contain a thorough description of the systems intended for inclusion in the eWAN authorization and the architecture to be used for the design and operation of the network. The description should contain the following details at a minimum:

- Currently authorized systems to be included in the eWAN ATO
- Region/State/City/CAGE code of all facilities to be included.
- Proposed network topology
- Method of transport security (e.g. CSfC, NSA Type 1 Encryptors)
- Supported Customers and Programs

2.4.1.1. Background

Content

An overview of the new or modified system to include as applicable, background, mission, objectives, and scope. In addition to providing the background for the proposed system, this section should provide a brief summary of the motivation for the system.

Examples of motivations for a system might include automation of certain tasks or taking advantage of new opportunities. The goals for the new or modified system should also be defined, together with the strategies, solutions, tactics, methods, and techniques proposed to achieve those goals.

Writing the Proposal, *Continued*

2.4.1.2. Objectives

Content

The system objectives reflect the business situation to be achieved with the NISP eWAN. Ideally the objectives support the intent to improve performance and security through better procedures and methods to support enterprise management and operations. The system analysis and design capture the outcomes or objectives relating to shaping organizations, improving performance to achieve business objectives.

2.4.1.3. Operational Policies & Constraints

Operational Policies

Each NISP eWAN will have numerous operational policies in place as the subordinate nodes, sites, and systems all have policies in place prior to eWAN development. The eWAN policies may be conglomerate documents based on the subordinate system policies incorporated.

The NISP eWAN initial analysis will analyze and evaluate subordinate site and system polices to ensure that the content supports eWAN operations and that eWAN operations support multisite system management and single site system instances as determined by the corporate responsible officer.

Constraints

The NISP eWAN constraints should be identified during the analysis. The constraints directly relate to the company business and operational strategies, technical and functional capabilities or limitations, and integration requirements to enable the system support and operation.

2.4.1.4. Scope

Objective

The system scope communicates the overall quantitative and qualitative system characteristics to the user, buyer, developer, and other organizational elements (e.g., training, facilities, staffing, and maintenance). It describes the user organization(s), mission(s), and organizational objectives from an integrated systems point of view.

Defining the system scope supports effective requirements development.

Writing the Proposal, *Continued*

2.4.1.1. User Classes & Other Involved Personnel

Overview

A user class is distinguished by the ways in which the users interact with the system. Factors that distinguish a user class include responsibilities, skill level, work activities, and mode of interaction with the system. Different user classes may have distinct operational scenarios (use cases) for their interactions with the system.

In this context, a user is anyone who will interact with the proposed system to include: operational users, data entry personnel, system operators, operational support personnel, software maintainers, and trainers. Each category should be described in subordinate subparagraphs. .

2.4.1.2. Support Environment

Content

The support concepts and support environment for the proposed system include the following: the support agency or agencies; facilities; equipment; support software; repair or replacement criteria; maintenance levels and cycles; and storage, distribution, and supply methods.

The eWAN support nodes, elements, manning plan, and processes are just a few of the concepts associated with the support environment, which will be unique to each company.

2.4.2. Design Strategy

Overview

The design strategy describes the approach to the eWAN project to include:

- Mode of development
- Model validation
- Simulation
- Control design and tuning
- Performance verification
- Others as applicable

If the project calls for additional subsystem developments, such as special-purpose sensors, mechanical components, etc., this should be discussed in the design approach to these subsystems.

Design alternatives may be considered and evaluation methodologies to evaluate the alternates as required. A block diagram or process workflow may be helpful to convey how different components and stages in the design fit together.

The design processes are proprietary to each company. The NISP eWAN design will be approved by the company. The Program Manager is available to support Industry questions.

Design Strategy, *Continued*

2.4.2.1. Design Plan of Action

Overview

The design plan of action captures the Industry specific approach and may address process steps similar to the following:

- Completion of the System Concept and functional analysis
- Assembling a System Design/Development Team
- Development of the System/eWAN Concept of Operations
- Refinement of functional and technical requirements
- Completion of preliminary designs
- Initiating the system development process

2.4.2.2. Verification Plan

Testing Procedures

Outline the test procedures for the eWAN project. This may include the resulting tables, graphs, and measured values that will assess the eWAN performance. The projected testing procedures may be at the enterprise; node; individual system, components and subsystems (e.g., model validation, sensor subsystem, etc.), and the overall system(s) as defined in the design specification, operation or support concept as projected within the operational concept.

2.4.2.3. Design Approval

Overview

The design review process and inputs will be specific to the Industry participant requesting an eWAN. A generic process may contain some of the following process steps:

- System Concept of Operations Review
- System Requirements Review and Approval
- eWAN Architecture review
- System Design Review
- System Build Plan Review
- Initial Test Plan Review
- System Design Approval

3.0 eWAN Implementation

Overview

The NISP eWAN development process results in a core build and a test plan. These process outputs are critical for the eWAN to achieve an Initial Authority To Test (IATT). During testing the company will be able to validate the functional requirements for performance and finalize the eWAN build via the testing process. It is important to note that under no circumstances may classified or program data be transmitted across the eWAN architecture during testing. Figure 3.1 provides a strategic view of a conceptual development process. The DSS Program Manager will coordinate and execute the eWAN Test Plan review. The NAO will make the IATT decision.

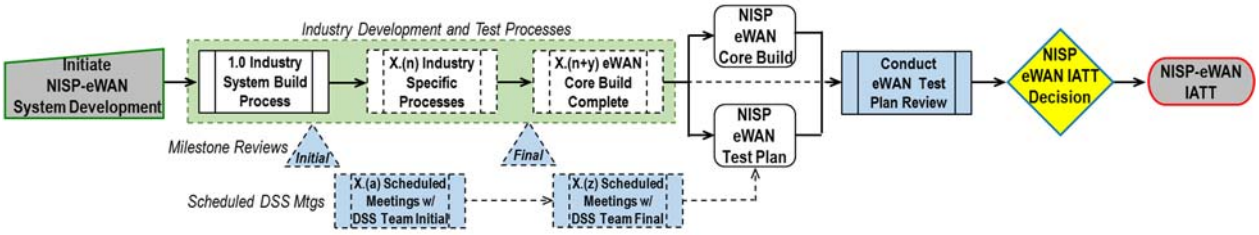

Figure 3.1 NISP eWAN Development Process
(Process Projection)

Program Manager Engagement

During the build process, the DSS Program Manager will be available for to support questions. Aligning engagements with milestones may be the advantageous use of time. As every NISP eWAN will be configured to meet each organizations business and operational objectives as the eWAN are designed to support management of a specific company's NISP systems. After the IATT is approved, the Cleared Industry will continue the build process in coordination with the DAAPM and other policy documents. After Industry complete the internal assessment and updates the eWAN system record in eMASS, ISSM of record may schedule the DSS assessment with the eWAN PM.

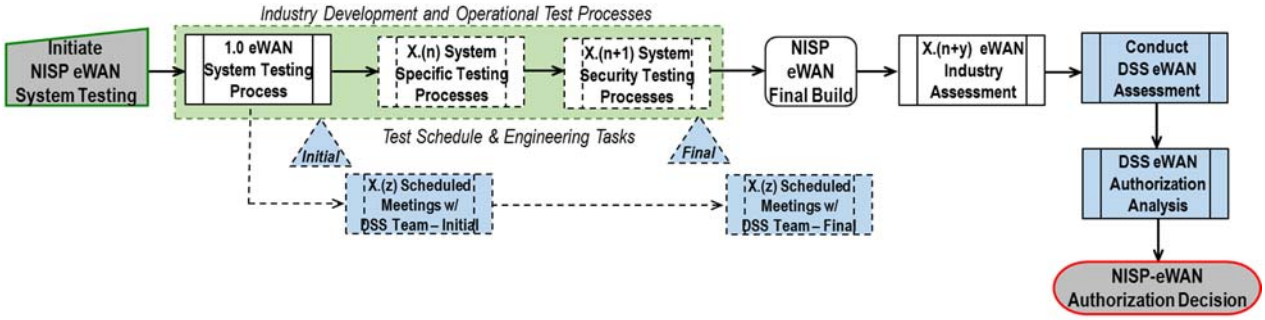

Figure 3.2 NISP eWAN Engineering and Risk Management Process
(Process Projection)

eWAN Implementation, *Continued*

DSS Assessment and Authorization	Industry participants developing NISP eWANs will create eMASS system records to support the Risk Management Framework tasks identified in the DSS Assessment and Authorization Process Manual (DAAPM). The NISP eMASS instance will be used to create eWAN system record and the ISSM of record will be responsible for the system artifact inputs and record management task leading up the system assessment. The DSS eWAN Program Manager will coordinate the eWAN assessment tasks to support the DSS RMF tasks and the onsite visit.
eWAN Annual Reviews	Industry participants developing NISP eWANs will create eMASS system records to support the Risk Management Framework tasks identified in the DSS Assessment and Authorization Process Manual (DAAPM). The NISP eMASS instance will be used to create eWAN system record and the ISSM of record will be responsible for the system artifact inputs and record management task leading up the system assessment.

This page intentionally left blank.