Unit #1c

MIS5214

Case Study 1 – The Titan Incident

Agenda

- Defense in Depth and Introduction to N-Tier Architecture
- Titan Case Study
- FedRAMP SSP and documentation of encryption related controls

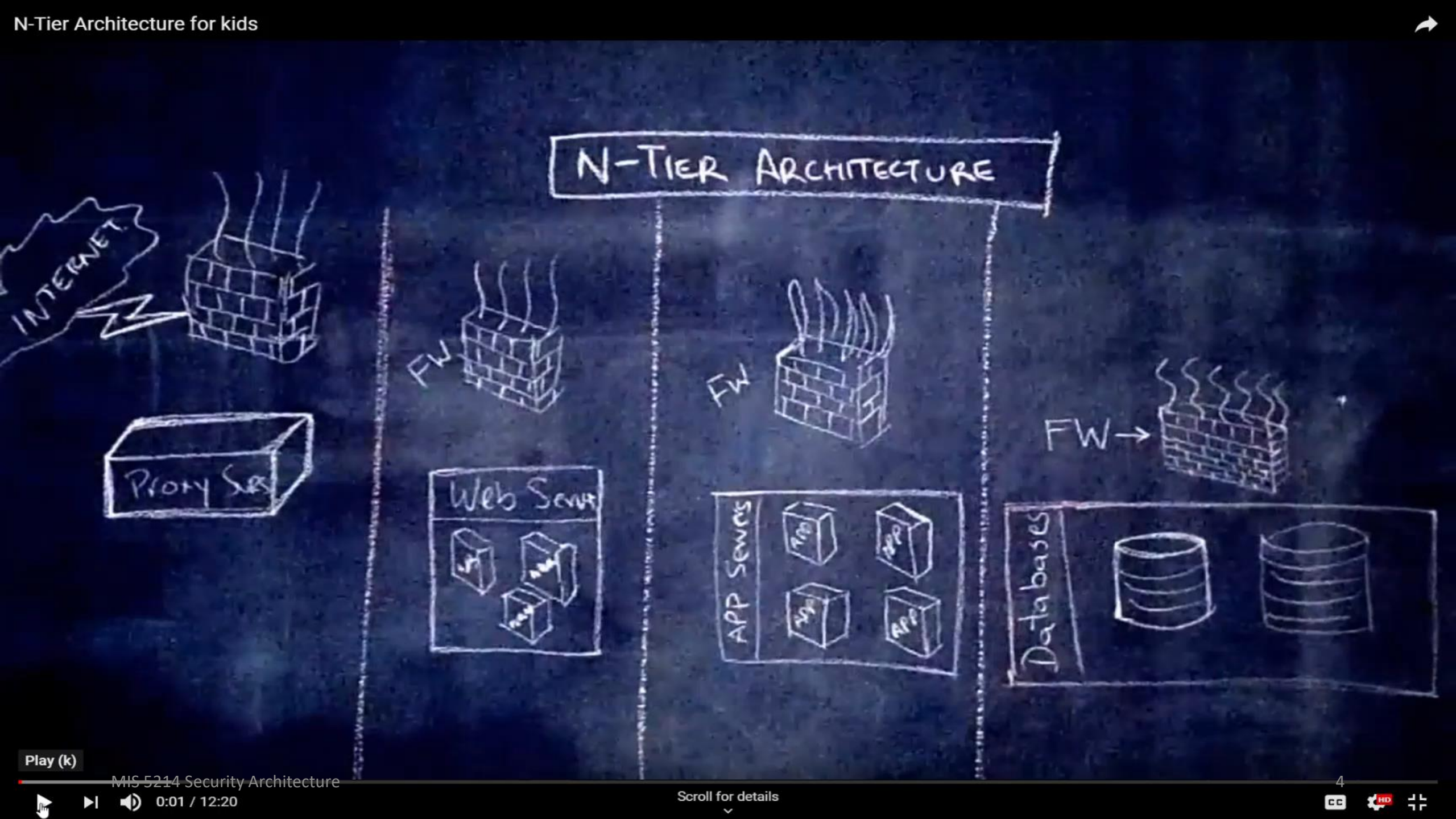
Important Security Architecture Model:

Defense in Depth

Also known as:

- Layered Security

We will studying elements of layered security moving forward…


N-Tier Architecture for kids
N-TIER ARCHITECTURE
INTERNET
FW
FW
FW
Web Servers
APP Servers
Databases
Play (k)
0:01 / 12:20
Scroll for details

Exercise: Draw an N-Tier Architecture for a Web-Based System

You can use www.draw.io, other graphic drawing program, or PowerPoint

- Consider a web-based system for managing the data of public utilities for a small town
- Identify who the users are
- Draw an N-Tier Architecture for the web-based system

Draw a logical network diagram for the Titan System - adding in graphical elements that illustrate the system boundary, interconnections and data flow

You can use www.draw.io, other graphic drawing program, or PowerPoint

Use your drawing to help you answer the following questions:

1. What was the specific attack vector(s) used by attacker?

2. What failings existed in the following areas?
   - IT Governance
   - End users
   - Information technology services
   - Information security
   - Incident response

Draw a logical network diagram adding in graphical elements that illustrate the system boundary, interconnections and data flow

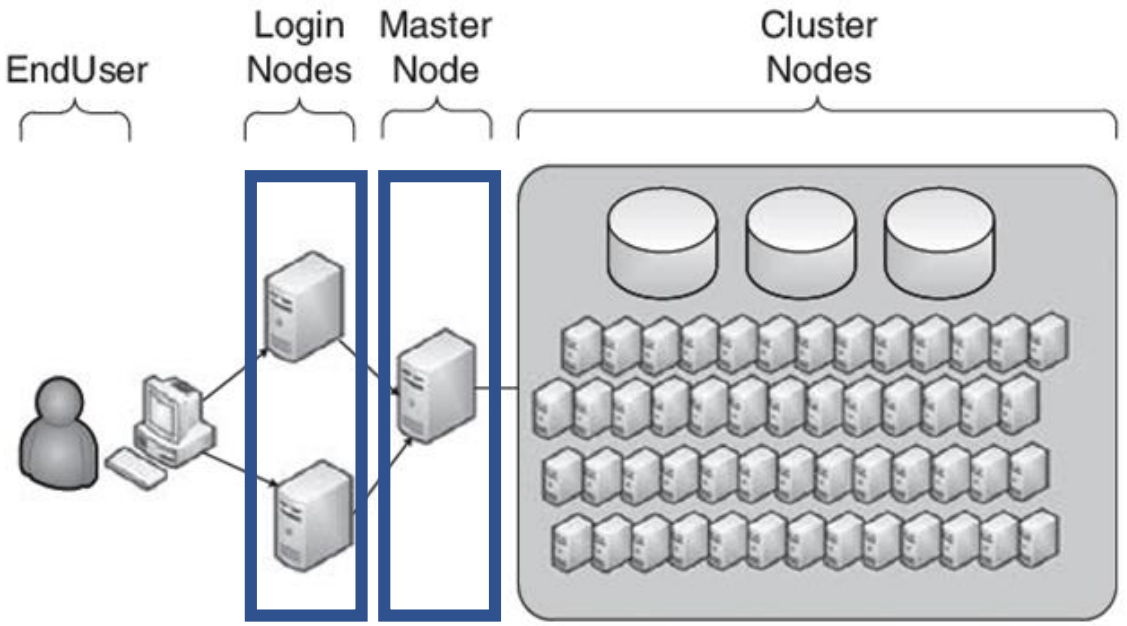


Figure 1 A typical grid architecture.

A High Performance Computing Cluster Under Attack: The Titan Incident

What was the specific attack vector(s) used by attacker:

1. ?
2. ?
3. ?
4. ?
5. ?
6. ?

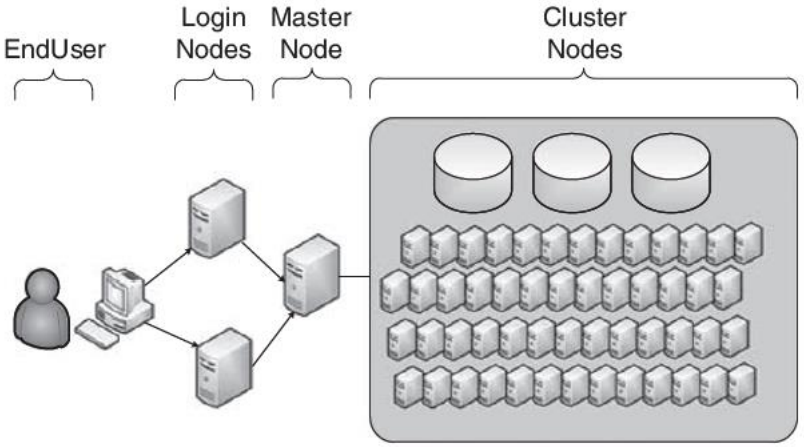


Figure 1 A typical grid architecture.

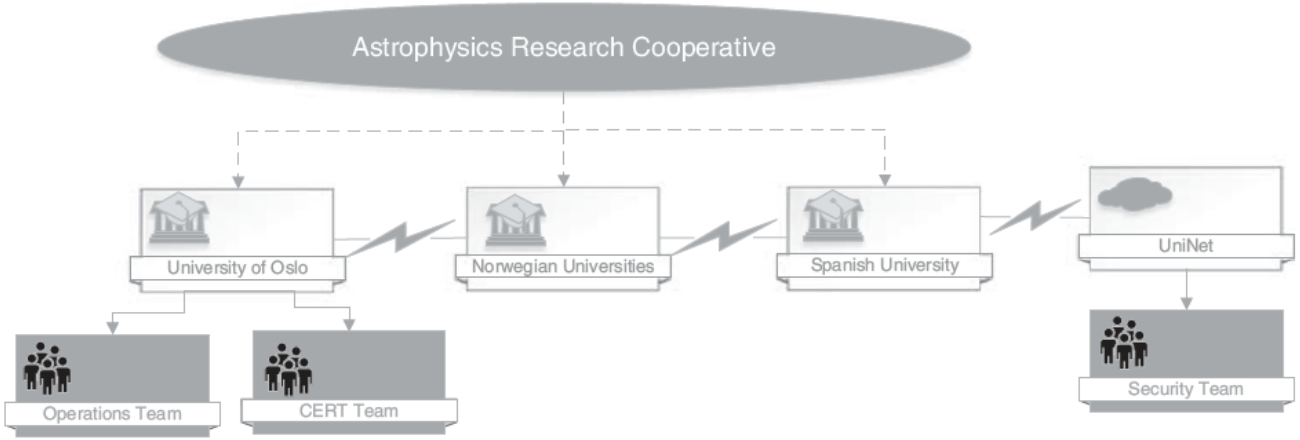


Figure 2 Geographic dispersion of Nordic DataGrid facility Tier-1 clusters.

A High Performance Computing Cluster Under Attack: The Titan Incident

Specific attack vector used by attacker:

1. Attacker obtained valid user names and password combinations from a system in Spain that had a research agreement with University of Oslo (UiO)
2. Attacker accessed the Titan cluster as a research user using the valid credentials that were “harvested” from the previously compromised system
3. The attacker used a local system exploit (CVE-2010-3847) to gain administrative privileges on the Titan system
4. Once administrative privileges were obtained, the attacker modified the SSH system files to collect the usernames and passwords of other end-users as they accessed the grid
5. The attacker created at least one “backdoor”, or method of accessing the system without relying on the compromised accounts
6. The newly stolen credentials were used to gain unauthorized access to other systems, and they may also have been sold on the black market

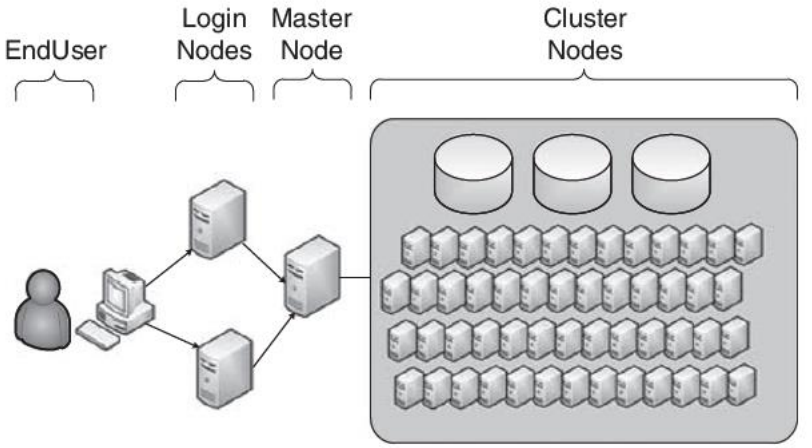


Figure 1 A typical grid architecture.

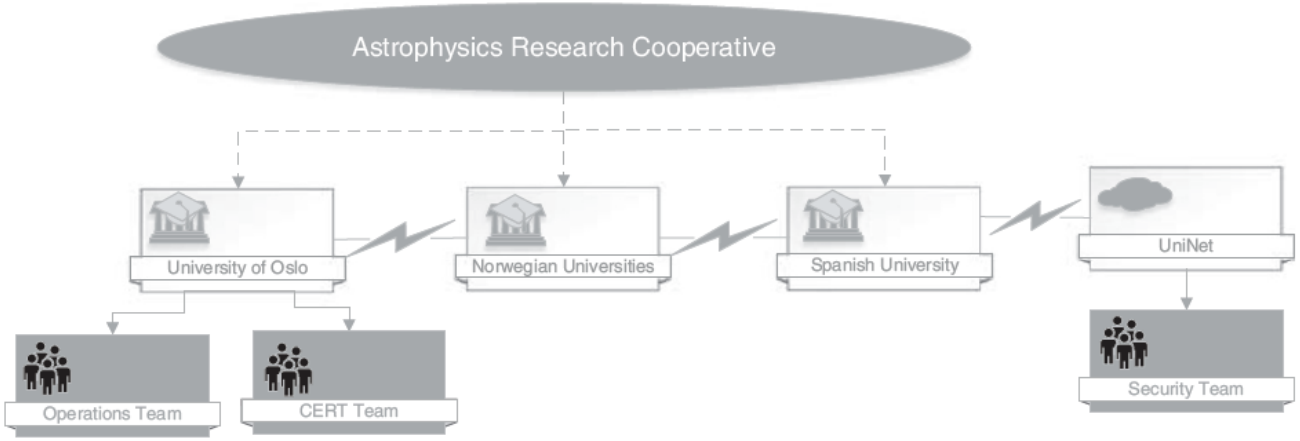
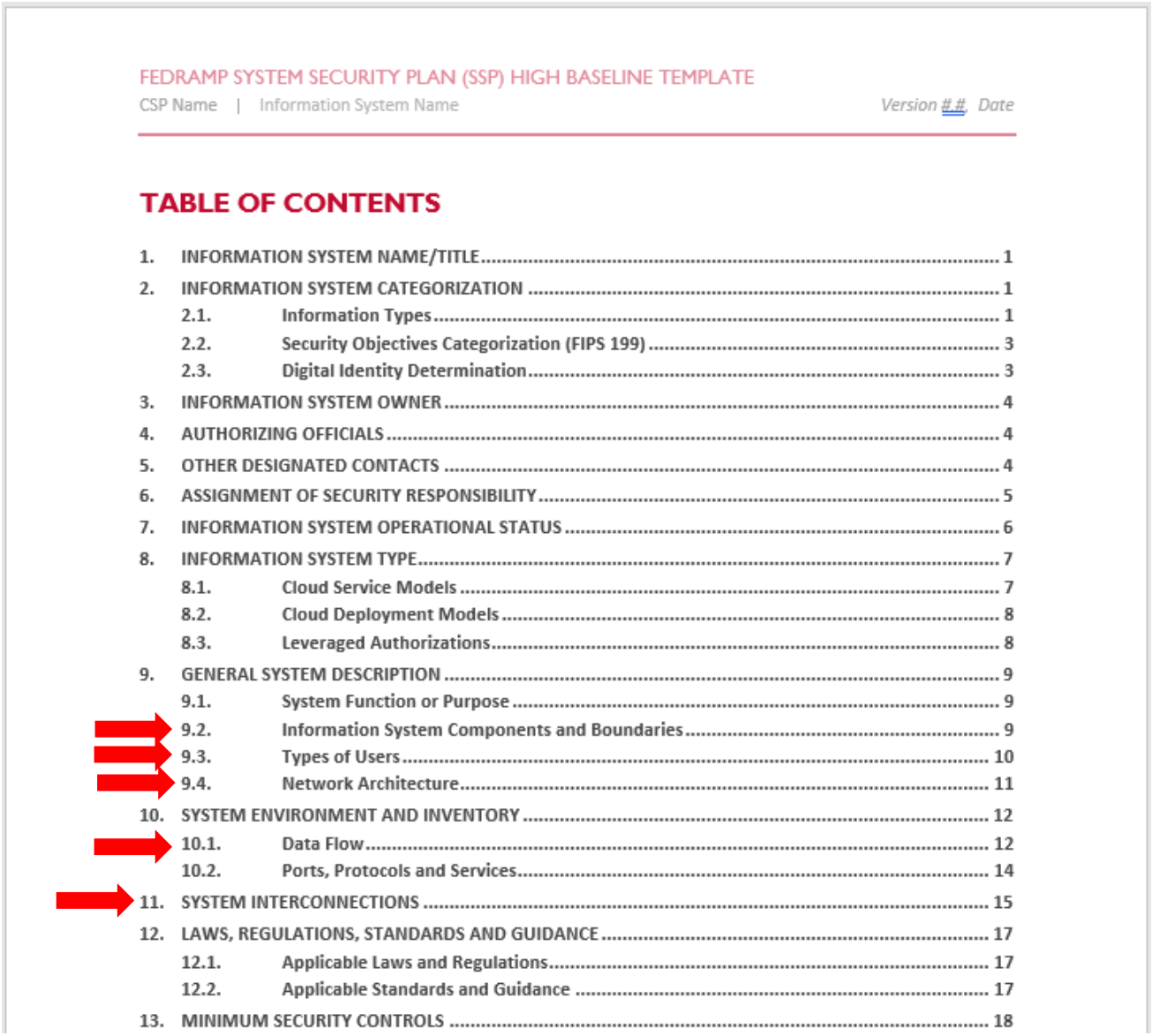


Figure 2 Geographic dispersion of Nordic DataGrid facility Tier-1 clusters.

What should Margrete Raaum do next?

	Preventive Controls	Detective Controls	Corrective/Responsive Controls
Information Security			
Incident Response			
IT Governance			

Where in the FedRAMP System Security Plan would you look for information to help you audit the security of the Titan Information System?



FEDRAMP SYSTEM SECURITY PLAN (SSP) HIGH BASELINE TEMPLATE

CSP Name | Information System Name *Version # #, Date*

TABLE OF CONTENTS

1. INFORMATION SYSTEM NAME/TITLE 1
2. INFORMATION SYSTEM CATEGORIZATION 1
   - 2.1. Information Types 1
   - 2.2. Security Objectives Categorization (FIPS 199) 3
   - 2.3. Digital Identity Determination 3
3. INFORMATION SYSTEM OWNER 4
4. AUTHORIZING OFFICIALS 4
5. OTHER DESIGNATED CONTACTS 4
6. ASSIGNMENT OF SECURITY RESPONSIBILITY 5
7. INFORMATION SYSTEM OPERATIONAL STATUS 6
8. INFORMATION SYSTEM TYPE 7
   - 8.1. Cloud Service Models 7
   - 8.2. Cloud Deployment Models 8
   - 8.3. Leveraged Authorizations 8
9. GENERAL SYSTEM DESCRIPTION 9
   - 9.1. System Function or Purpose 9
   - 9.2. Information System Components and Boundaries 9
   - 9.3. Types of Users 10
   - 9.4. Network Architecture 11
10. SYSTEM ENVIRONMENT AND INVENTORY 12
    - 10.1. Data Flow 12
    - 10.2. Ports, Protocols and Services 14
11. SYSTEM INTERCONNECTIONS 15
12. LAWS, REGULATIONS, STANDARDS AND GUIDANCE 17
    - 12.1. Applicable Laws and Regulations 17
    - 12.2. Applicable Standards and Guidance 17
13. MINIMUM SECURITY CONTROLS 18

…the attacker modified SSH system files to collect the usernames and passwords of other end-users as they accessed the grid

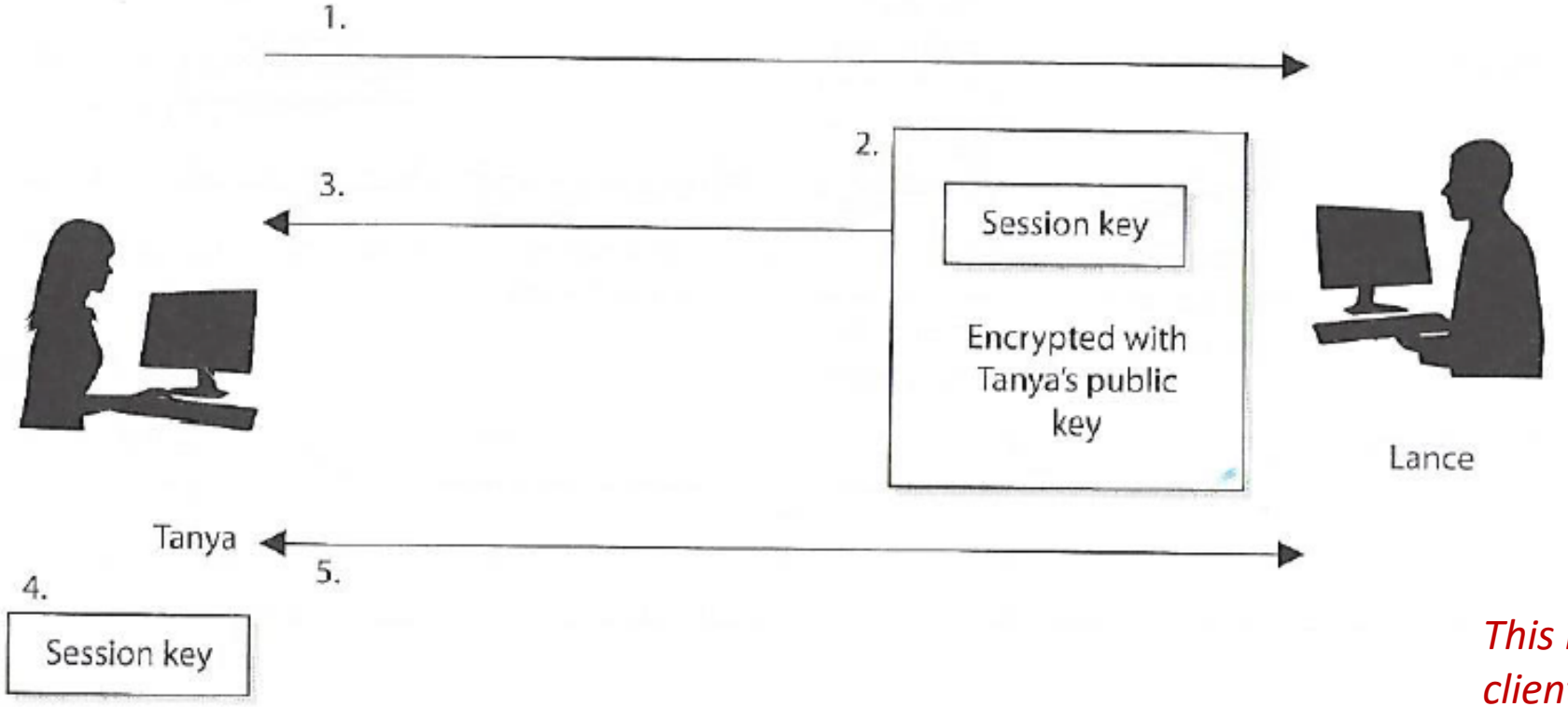
Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. SSH provides a secure channel over an unsecured network in a client-server architecture, connecting an SSH client application with an SSH server

> Common applications include remote command-line login and remote command execution, but any network service can be secured with SSH. The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-2.

The most visible application of the protocol is for access to shell accounts on Unix-like operating systems, but is in limited use on Windows as well

Remember… Session keys ?

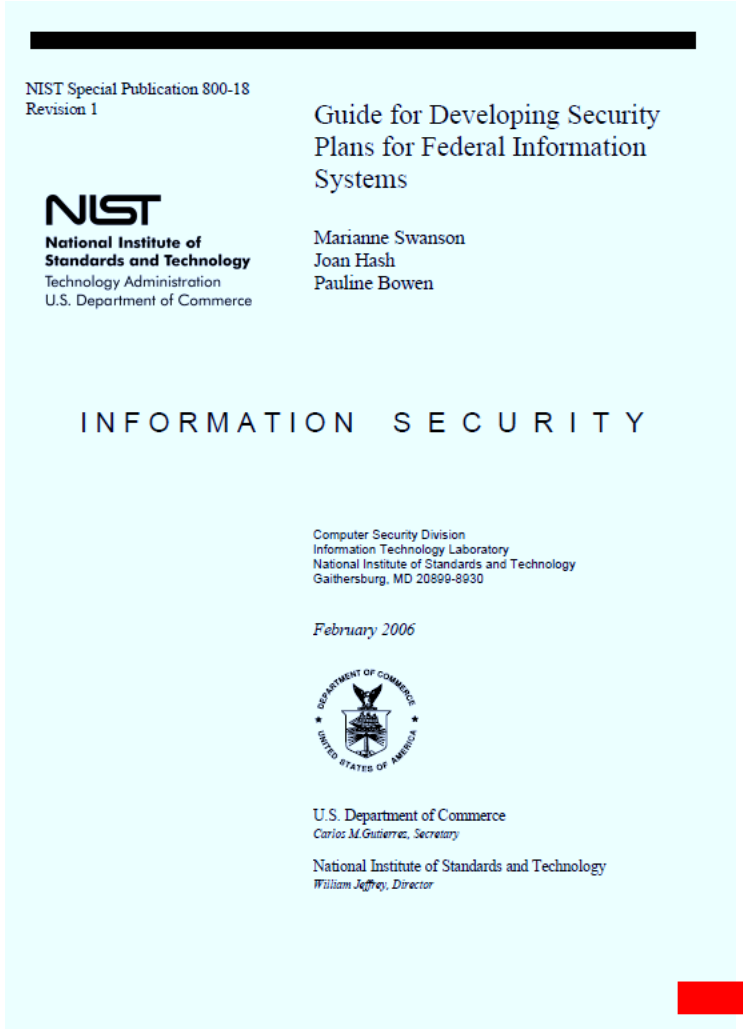
Single-use symmetric keys used to encrypt messages between two users in an individual communication session



1) Tanya sends Lance her public key.
2) Lance generates a random session key and encrypts it using Tanya's public key.
3) Lance sends the session key, encrypted with Tanya's public key, to Tanya.
4) Tanya decrypts Lance's message with her private key and now has a copy of the session key.
5) Tanya and Lance use this session key to encrypt and decrypt messages to each other.

This is how secure web client applications communicate with server-side services

Where do you look for encryption related controls that could help Titan?



NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Marianne Swanson
Joan Hash
Pauline Bowen

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2006

U.S. Department of Commerce
Carlos M.Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
System and Communications Protection					
SC-1	System and Communications Protection Policy and Procedures	P1	SC-1	SC-1	SC-1
SC-2	Application Partitioning	P1	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	P1	Not Selected	Not Selected	SC-3
SC-4	Information in Shared Resources	P1	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	P1	SC-5	SC-5	SC-5
SC-6	Resource Availability	P0	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	P1	SC-7	SC-7 (3) (4) (5) (7)	SC-7 (3) (4) (5) (7) (8) (18) (21)
SC-8	Transmission Confidentiality and Integrity	P1	Not Selected	SC-8 (1)	SC-8 (1)
SC-9	**Withdrawn**	---	---	---	---
SC-10	Network Disconnect	P2	Not Selected	SC-10	SC-10
SC-11	Trusted Path	P0	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	P1	SC-12	SC-12	SC-12 (1)
SC-13	Cryptographic Protection	P1	SC-13	SC-13	SC-13
SC-14	**Withdrawn**	---	---	---	---
SC-15	Collaborative Computing Devices	P1	SC-15	SC-15	SC-15
SC-16	Transmission of Security Attributes	P0	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	P1	Not Selected	SC-17	SC-17
SC-18	Mobile Code	P2	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	P1	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	SC-20	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	SC-22	SC-22	SC-22
SC-23	Session Authenticity	P1	Not Selected	SC-23	SC-23
SC-24	Fail in Known State	P1	Not Selected	Not Selected	SC-24
SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28
SC-39	Process Isolation	P1	SC-39	SC-39	SC-39

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*].

Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems. Related controls: SC-13, SC-17.

Control Enhancements:

(1) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY*

The organization maintains availability of information in the event of the loss of cryptographic keys by users.

Supplemental Guidance: Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys (e.g., due to forgotten passphrase).

(2) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS*

The organization produces, controls, and distributes symmetric cryptographic keys using [*Selection: NIST FIPS-compliant; NSA-approved*] key management technology and processes.

(3) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS*

The organization produces, controls, and distributes asymmetric cryptographic keys using [*Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key*].

(4) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES*

[Withdrawn: Incorporated into SC-12].

(5) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES / HARDWARE TOKENS*

[Withdrawn: Incorporated into SC-12].

References: NIST Special Publications 800-56, 800-57.

Priority and Baseline Allocation:

P1	**LOW** SC-12	**MOD** SC-12	**HIGH** SC-12 (1)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
System and Communications Protection					
SC-1	System and Communications Protection Policy and Procedures	P1	SC-1	SC-1	SC-1
SC-2	Application Partitioning	P1	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	P1	Not Selected	Not Selected	SC-3
SC-4	Information in Shared Resources	P1	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	P1	SC-5	SC-5	SC-5
SC-6	Resource Availability	P0	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	P1	SC-7	SC-7 (3) (4) (5) (7)	SC-7 (3) (4) (5) (7) (8) (18) (21)
SC-8	Transmission Confidentiality and Integrity	P1	Not Selected	SC-8 (1)	SC-8 (1)
SC-9	**Withdrawn**	---	---	---	---
SC-10	Network Disconnect	P2	Not Selected	SC-10	SC-10
SC-11	Trusted Path	P0	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	P1	SC-12	SC-12	SC-12 (1)
SC-13	Cryptographic Protection	P1	SC-13	SC-13	SC-13
SC-14	**Withdrawn**	---	---	---	---
SC-15	Collaborative Computing Devices	P1	SC-15	SC-15	SC-15
SC-16	Transmission of Security Attributes	P0	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	P1	Not Selected	SC-17	SC-17
SC-18	Mobile Code	P2	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	P1	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	SC-20	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	SC-22	SC-22	SC-22
SC-23	Session Authenticity	P1	Not Selected	SC-23	SC-23
SC-24	Fail in Known State	P1	Not Selected	Not Selected	SC-24
SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28
SC-39	Process Isolation	P1	SC-39	SC-39	SC-39

SC-13 CRYPTOGRAPHIC PROTECTION

Control: The information system implements [*Assignment: organization-defined cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Supplemental Guidance: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.

Control Enhancements: None.

(1) *CRYPTOGRAPHIC PROTECTION | FIPS-VALIDATED CRYPTOGRAPHY*
[Withdrawn: Incorporated into SC-13].

(2) *CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY*
[Withdrawn: Incorporated into SC-13].

(3) *CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS*
[Withdrawn: Incorporated into SC-13].

(4) *CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES*
[Withdrawn: Incorporated into SC-13].

References: FIPS Publication 140; Web: http://csrc.nist.gov/cryptval, http://www.cnss.gov.

Priority and Baseline Allocation:

P1	**LOW** SC-13	**MOD** SC-13	**HIGH** SC-13

SC-13 CRYPTOGRAPHIC PROTECTION

Control: The information system implements [*Assignment: organization-defined cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Supplemental Guidance: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.

Control Enhancements: None.

(1) *CRYPTOGRAPHIC PROTECTION | FIPS-VALIDATED CRYPTOGRAPHY*
[Withdrawn: Incorporated into SC-13].

(2) *CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY*
[Withdrawn: Incorporated into SC-13].

(3) *CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS*
[Withdrawn: Incorporated into SC-13].

(4) *CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES*
[Withdrawn: Incorporated into SC-13].

References: FIPS Publication 140; Web: http://csrc.nist.gov/cryptval, http://www.cnss.gov.

Priority and Baseline Allocation:

P1	**LOW** SC-13	**MOD** SC-13	**HIGH** SC-13

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Where do you document this information in your SSP?

TABLE OF CONTENTS

1. INFORMATION SYSTEM NAME/TITLE 1
2. INFORMATION SYSTEM CATEGORIZATION 1
2.1. Information Types 1
2.2. Security Objectives Categorization (FIPS 199) 3
2.3. Digital Identity Determination 3
3. INFORMATION SYSTEM OWNER 4
4. AUTHORIZING OFFICIALS 4
5. OTHER DESIGNATED CONTACTS 4
6. ASSIGNMENT OF SECURITY RESPONSIBILITY 5
7. INFORMATION SYSTEM OPERATIONAL STATUS 6
8. INFORMATION SYSTEM TYPE 7
8.1. Cloud Service Models 7
8.2. Cloud Deployment Models 8
8.3. Leveraged Authorizations 8
9. GENERAL SYSTEM DESCRIPTION 9
9.1. System Function or Purpose 9
9.2. Information System Components and Boundaries 9
9.3. Types of Users 10
9.4. Network Architecture 11
10. SYSTEM ENVIRONMENT AND INVENTORY 12
10.1. Data Flow 12
10.2. Ports, Protocols and Services 14
11. SYSTEM INTERCONNECTIONS 15
12. LAWS, REGULATIONS, STANDARDS AND GUIDANCE 17
12.1. Applicable Laws and Regulations 17
12.2. Applicable Standards and Guidance 17
13. MINIMUM SECURITY CONTROLS 18
13.1. Access Control (AC) 25
AC-1 Access Control Policy and Procedures Requirements (H) 25
AC-2 Account Management (H) 26
AC-2 (1) Control Enhancement (M) (H) 27
AC-2 (2) Control Enhancement (H) 28
AC-2 (3) Control Enhancement (H) 29
AC-2 (4) Control Enhancement (H) 30
AC-2 (5) Control Enhancement (H) 31
AC-2 (7) Control Enhancement (H) 31
AC-2 (9) Control Enhancement (H) 32
AC-2 (10) Control Enhancement (M) (H) 33
AC-2 (11) Control Enhancement (H) 34
AC-2 (12) Control Enhancement (H) 35

FEDRAMP SYSTEM SECURITY PLAN (SSP) HIGH BASELINE TEMPLATE

Cloud Service Provider Name

Information System Name

Version #

Version Date

FedRAMP

CONTROLLED UNCLASSIFIED INFORMATION

SA-9 (5) Control Enhancement (M) (H) 315
SA-10 Developer Configuration Management (M) (H) 316
SA-10 (1) Control Enhancement (M) (H) 317
SA-11 Developer Security Testing and Evaluation (M) (H) 318
SA-11 (1) Control Enhancement (M) (H) 319
SA-11 (2) Control Enhancement (M) (H) 320
SA-11 (8) Control Enhancement (M) (H) 321
SA-12 Supply Chain Protection (H) 322
SA-15 Development Process, Standards, and Tools (H) 322
SA-16 Developer-Provided Training (H) 324
SA-17 Developer Security Architecture and Design (H) 324
13.16. System and Communications Protection (SC) 325
SC-1 System and Communications Protection Policy and Procedures (H) 325
SC-2 Application Partitioning (M) (H) 326
SC-3 Security Function Isolation (H) 327
SC-4 Information in Shared Resources (M) (H) 328
SC-5 Denial of Service Protection (L) (M) (H) 329
SC-6 Resource Availability (M) (H) 329
SC-7 Boundary Protection (L) (M) (H) 330
SC-7 (3) Control Enhancement (M) (H) 331
SC-7 (4) Control Enhancement (H) 332
SC-7 (5) Control Enhancement (M) (H) 333
SC-7 (7) Control Enhancement (M) (H) 334
SC-7 (8) Control Enhancement (M) (H) 335
SC-7 (10) Control Enhancement (H) 335
SC-7 (12) Control Enhancement (H) 336
SC-7 (13) Control Enhancement (H) 337
SC-7 (18) Control Enhancement (M) (H) 338
SC-7 (20) Control Enhancement (H) 339
SC-7 (21) Control Enhancement (H) 339
SC-8 Transmission confidentiality and Integrity (M) (H) 340
SC-8 (1) Control Enhancement (M) (H) 341
SC-10 Network Disconnect (H) 342
SC-12 Cryptographic Key Establishment & Management (L) (M) (H) 343
SC-12 (1) Control Enhancement (H) 344
SC-12 (2) Control Enhancement (M) (H) 344
SC-12 (3) Control Enhancement (M) (H) 345
SC-13 Use of Cryptography (L) (M) (H) 346
SC-15 Collaborative Computing Devices (M) (H) 347
SC-17 Public Key Infrastructure Certificates (M) (H) 348
SC-18 Mobile Code (M) (H) 349
SC-19 Voice Over Internet Protocol (M) (H) 350
SC-20 Secure Name / Address Resolution Service (Authoritative Source) (L) (M) (H) 351
SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) (L) (M) (H) 352
SC-22 Architecture and Provisioning for Name / Address Resolution Service (L) (M) (H) 353
SC-23 Session Authenticity (M) (H) 353

SC-12 Cryptographic Key Establishment & Management (L) (M) (H)

The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*].

SC-12 Additional FedRAMP Requirements and Guidance:

Guidance: Federally approved and validated cryptography.

SC-12	Control Summary Information
Responsible Role:	
Parameter SC-12:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

SC-12 What is the solution and how is it implemented?

SA-9 (5) Control Enhancement (M) (H) 315
SA-10 Developer Configuration Management (M) (H) 316
SA-10 (1) Control Enhancement (M) (H) 317
SA-11 Developer Security Testing and Evaluation (M) (H) 318
SA-11 (1) Control Enhancement (M) (H) 319
SA-11 (2) Control Enhancement (M) (H) 320
SA-11 (8) Control Enhancement (M) (H) 321
SA-12 Supply Chain Protection (H) 322
SA-15 Development Process, Standards, and Tools (H) 322
SA-16 Developer-Provided Training (H) 324
SA-17 Developer Security Architecture and Design (H) 324
13.16. System and Communications Protection (SC) 325
SC-1 System and Communications Protection Policy and Procedures (H) 325
SC-2 Application Partitioning (M) (H) 326
SC-3 Security Function Isolation (H) 327
SC-4 Information in Shared Resources (M) (H) 328
SC-5 Denial of Service Protection (L) (M) (H) 329
SC-6 Resource Availability (M) (H) 329
SC-7 Boundary Protection (L) (M) (H) 330
SC-7 (3) Control Enhancement (M) (H) 331
SC-7 (4) Control Enhancement (H) 332
SC-7 (5) Control Enhancement (M) (H) 333
SC-7 (7) Control Enhancement (M) (H) 334
SC-7 (8) Control Enhancement (M) (H) 335
SC-7 (10) Control Enhancement (H) 335
SC-7 (12) Control Enhancement (H) 336
SC-7 (13) Control Enhancement (H) 337
SC-7 (18) Control Enhancement (M) (H) 338
SC-7 (20) Control Enhancement (H) 339
SC-7 (21) Control Enhancement (H) 339
SC-8 Transmission confidentiality and Integrity (M) (H) 340
SC-8 (1) Control Enhancement (M) (H) 341
SC-10 Network Disconnect (H) 342
SC-12 Cryptographic Key Establishment & Management (L) (M) (H) 343
SC-12 (1) Control Enhancement (H) 344
SC-12 (2) Control Enhancement (M) (H) 344
SC-12 (3) Control Enhancement (M) (H) 345
SC-13 Use of Cryptography (L) (M) (H) 346
SC-15 Collaborative Computing Devices (M) (H) 347
SC-17 Public Key Infrastructure Certificates (M) (H) 348
SC-18 Mobile Code (M) (H) 349
SC-19 Voice Over Internet Protocol (M) (H) 350
SC-20 Secure Name / Address Resolution Service (Authoritative Source) (L) (M) (H) 351
SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) (L) (M) (H) 352
SC-22 Architecture and Provisioning for Name / Address Resolution Service (L) (M) (H) 353
SC-23 Session Authenticity (M) (H) 353

SC-12 (1) CONTROL ENHANCEMENT (H)
The organization maintains availability of information in the event of the loss of cryptographic keys by users.

SC-12 (2) CONTROL ENHANCEMENT (M) (H)
The organization produces, controls, and distributes symmetric cryptographic keys using [FedRAMP Selection: NIST FIPS-compliant] key management technology and processes.

SC-12 (3) CONTROL ENHANCEMENT (M) (H)
The organization produces, controls, and distributes asymmetric cryptographic keys using [Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key].

SC-13 Use of Cryptography (L) (M) (H)
The information system implements [FedRAMP Assignment: FIPS-validated or NSA-approved cryptography] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Agenda

- ✓Defense in Depth and Introduction to N-Tier Architecture
- ✓Titan Case Study
- ✓FedRAMP SSP and documentation of encryption related controls