NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

LEO Satellite Cyber Security Framework

EG|CERT
EGYPTIAN COMPUTER EMERGENCY READINESS TEAM

TLP: WHITE

The Traffic light Protocol (TLP)

The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s). The protocol includes four colors (traffic lights), which are detailed as follows:

Red- Not for disclosure, restricted to participants only:
Sources may use TLP: RED when information cannot be effectively acted upon by additional parties. Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed

Amber- Limited disclosure, restricted to participants' organizations:

Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

Green- Limited disclosure, restricted to the community:

Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

White- Disclosure is not limited:
Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. TLP: WHITE information may be distributed without restriction.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

Overview

The ability to connect to the internet is increasingly becoming a human necessity. All you have to do is look at how much time you spend on the internet on a daily basis to realize this. During the previous two years, the pandemic has proved how critical internet access is to our professional, social, and personal lives, and many companies and trades have become internet-dependent.

LEO Satellite Internet is not a new technology, but advances in other space-related technologies have resulted in a huge leap in its evolution, allowing it to scale and become a viable, affordable option for regular Internet users. Such a technology is very likely to cause a radical change in the global telecommunications market.

The National Telecom Regulatory Authority (NTRA) is the official authority in the Arab Republic of Egypt (ARE) for communication sector regulations, and it is in charge of issuing certifications and approvals to companies and organizations that want to provide communication-related solutions and services.

The new network with its global reach needs protection, which is a very complicated task to do due to the complex nature of the ecosystem that we want to secure.

Because of the increasing number of satellite internet operators such as StarLink, OneWeb, and Telesat, and because it is the NTRA's responsibility to ensure that people and organizations can benefit from satellite internet features such as availability, wide coverage, and low cost with privacy and safety, The NTRA realized that providing a set of baseline security guidelines framework for satellite internet service provider organizations is critical. To ensure that satellite internet services, systems, and facilities are safe, and the data privacy is adhered to in accordance with the Arab Republic of Egypt's regulations. The NTRA has studied the LEO Satellite internet security standards and guidelines that are relevant, applicable and effective in the ARE.

According to law 10 of year 2003 for telecom regulation, it is decided to publish this LEO satellite internet security guidelines framework in the ARE. This framework brings together most effective LEO satellite internet security guidelines and security assurance processes, in a sincere attempt to help satellite internet service providers for securing their systems, users and organizations by following a clear set of guidelines, which ensure to have required the security considerations and mitigating of most known attacks. The target is to guide consumers and organizations to get benefit from their LEO satellite internet devices and services securely, safely and privately.

Target Audience

Who is this document for?

LEO satellite internet service provider companies/organizations that are currently running, deploying, operating, providing or plan to run, deploy, operate, provide Satellite internet device, system, service, solution in the ARE. are obligated to obey the LEO satellite internet security guidelines outlined in this document.

LEO satellite internet service provider are companies or organizations that provide commercial services and solutions required by the LEO internet-based connectivity systems to operate. This includes satellite vehicles, networks, cloud storage, data transfer and any other service required for the full satellite internet solution.

Document Structure

The remainder of this document consists of the following sections and appendices:

- **Section 2** presents the definitions of terms and acronyms used in this document.
- **Section 3** presents the LEO satellite internet cybersecurity framework procedures
- **Section 4** includes references that aid in the creation of this text.
- **Section 5** contains the document's edit history.
- **Appendix A**: demonstrates the use of the LEO satellite internet security framework through live case study.
- **Appendix B**: contains more detailed descriptions for the controls that an organization should comply with in order to start deploying LEO satellite internet system in ARE.
- **Appendix C**: is a questionnaire that should be filled by the service provider

DEFINITION OF TERMS AND ACRONYMS

This section contains a brief explanation of the terms and abbreviations used in this document

Terms and definitions

LEO satellite	A piece of electronic equipment that orbits the Earth at a height of 160 to 2000 kilometers to accomplish a particular service or mission.
LEO satellite internet	A service/system that allows users to connect to internet using satellite vehicles that orbits in LEO
Satellite constellation	Number of similar satellites with similar types and functions designated to be in the same earth orbit that serve a shared purpose
Attack surface	All possible points (attack vectors), where an unauthorized user can access a system.
Attack vector	The method which a cyber attacker uses to gain unauthorized access to the system.
LEO satellite internet service providers	Company/organization that utilizing the LEO satellite constellations to provide internet connection with wide coverage and high speed.
The framework	Whenever stated in this document, it means the LEO satellite internet security guidelines framework in the ARE.
Responsible entity	The entity, vendor or service provider, which is responsible for considering and maintaining a specific security guideline.
Threat	An problem that could harm the system.
Vulnerabilities	The ways in which assets can be exploited.
Risk	The potential for loss or damage when a threat exploits a vulnerability.

Acronyms

ARE	Arab republic of Egypt
NTRA	National Telecom Regulatory Authority
NIST	The National Institute of Standards & Technology
LEO	Low Orbit Satellite
GS	Gateway Station
OWASP	Open Web Application Security Project
OMCS	Operation Management and Control System
MCS	Management and Control System
NMS	Network Management System
SCF	Cyber Security Framework

LEO SATELLITE CYBER SECURITY FRAMEWORK

About the framework

The LEO satellite internet cybersecurity framework (LEO – SI– CSF) is designed to offer LEO satellite internet suppliers and service providers with the necessary security rules and requirements. These guidelines compile the most effective LEO satellite internet security considerations in the field, which are applicable and conform with the ARE's satellite internet market's regulations and security requirements.

The framework should be used by LEO Satellite internet service providers, who intend to run, deploy, operate, provide a satellite internet device, system, service, solution in the ARE, to help them ensure that their products and provided services are secure enough and eligible (from a security perspective) for the market in the ARE.

LEO satellite internet security assurance process

The LEO satellite internet cybersecurity framework provides a set of security requirements to be complied by LEO satellite internet service providers. This section describes the LEO satellite internet security assurance process where the responsible entity should consider in order to assess the security of the LEO satellite internet systems or service. The responsible entity should adhere this process to determine whether the LEO satellite internet solution under consideration complies with the baseline security requirements or not.

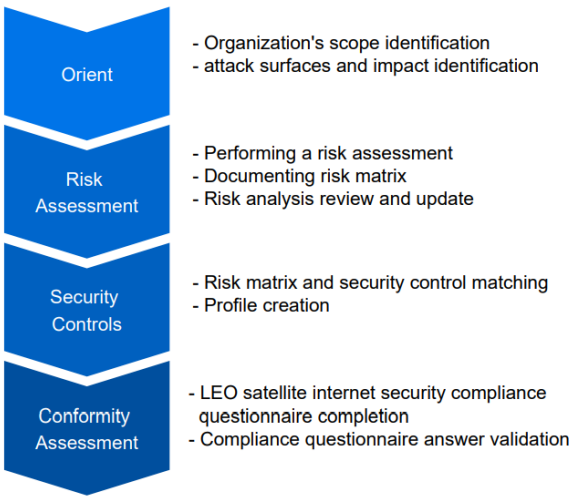


Figure 1 - LEO satellite internet CSF. assurance process

The assurance process consists of a set of four sequential activities, required to be performed by the responsible entity (organization/company), as demonstrated in Figure 1.

The LEO satellite internet CSF assurance process starts by orienting the organization to the scope of interest. The outcome of this operation is an asset identification table which contains a list of the organizational scope of operation. The organization’s assets and critical systems must be protect to ensure safe, secure, and reliable operation.

For the purpose of risk assessment, the asset identification table is then updated by adding the attack surface that exists in each critical system. The potential threat and the impact on the organization is then added to each attack surface. After that, the impact is categorized to determine the level of damage whether it affects a single piece of equipment, the whole network, or the national security. Then a likelihood and severity levels are assigned to each threat, which forms a risk register. The risk register is a list containing each threat, the impact level of the threat, threat likelihood and the impact category.

For the security controls step, the risk register is used to assign the mitigations to each potential threat as proposed by NIST cyber security framework (CSF). This functionality is used to overcome the threat before an incident (i.e., identify, protect), during an incident (i.e., detect, respond) or after an incident (i.e., recover). The outcomes of this step is a security class table that contains the potential threat and the corresponding functionalities needed to be carried out for mitigating such threat based on the risk level in the risk register.

The security class table is then utilized to formulate the organization's security profile, which is a list of security controls that match the mitigation functionalities implemented by the organization.

The security profile is then used for filling the questionnaire conformity assessment step to provide the evidences and responses. This determines whether the organization complies with the requirements or not. An organization should consider answering all questions applicable to the scope determined in the "Orient" step. It should provide reasons and evidence for their answers whenever possible. In this context, the resultant checklist clearly determines whether the LEO satellite internet solution complies with the security baseline or not.

ORIENT

Orient is the activity of identifying the organization's scope of operations, the scope of operations is the segment in which the organizations own, control and operates the assets that are used to operate satellite internet system. The satellite internet system is divided into three segments: ***space segment***, ***ground segment*** and ***user segment*** as demonstrated in Figure 2.

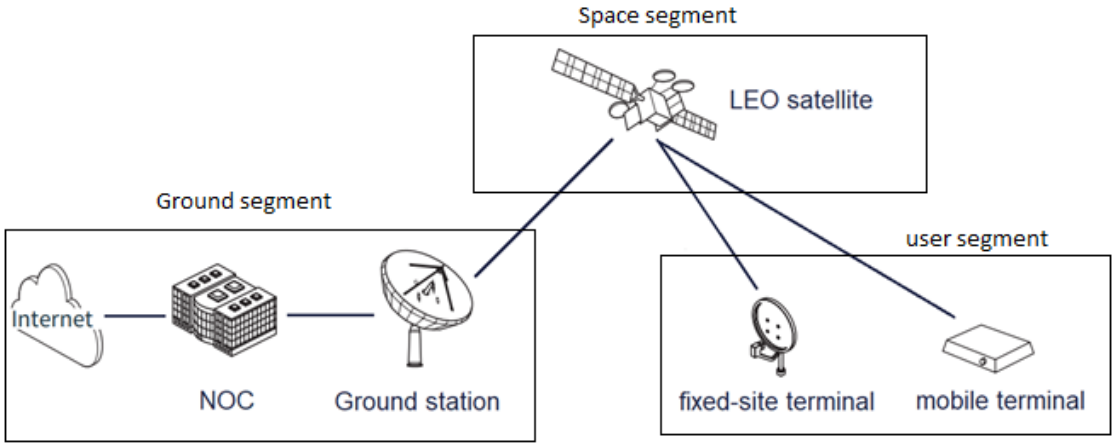


Figure 2 - Satellite internet solution segments

These segments represent the key points - attack surfaces - of satellite access. Table 1 shows a detailed explanation of the included utilities, devices, systems, functionalities and communication techniques used

to communicate with other segments. This helps in identifying the critical systems of each segment and the attack surfaces that could cause data leakage or even damage to the system if exploited by an attacker.

Table 1 – LEO satellite internet segments and assets

Segment name	Functionality	Included assets
Space segment **[1]**	The basic functionality of the space segment is to provide satellite-based connectivity by routing data and control signals to other satellites, ground stations that is connected through terrestrial network to the internet, command and control stations or to user's devices the space segment contains LEO satellite constellations which can be classified as constellations with ISL or constellations without ISL. the ISL "inter-satellite link" is the RF link that allows the satellite-to-satellite communication	- Satellite vehicle - Inter-satellite link communications - Satellite constellation
Ground segment **[2]**	This segment is responsible for issuing commands to a satellite control data handling platform and receives telemetry from a space vehicle The devices and systems included in this segment are also responsible for sending / receiving data packets to / from user to provide internet connectivity through RF link named feeder link	- Infrastructure networking system - Mission operation center (MOC) o Mission management o Bus command and control o Data processing and distribution o Payload control center - Ground station terminals (GS) o Data handling and routing o Space/ground communication - Mobile ground element
User segment **[3]**	This segment provides internet connectivity to users through fixed or portable devices named (satellite terminal) these devices communicate directly to the satellite vehicles via narrow or wide RF beam either by sending uplink signals to satellite or receiving downlink signals from it.	- Satellite terminal (ST) o Fixed-site terminal o Mobile terminal

The scope and assets identification help in the identification of critical systems included in each scope which will form the asset identification table.

A system is considered critical when it threats a human life, causes service outage, critical data leak, or threats critical infrastructure when compromised. "Failure" in this context does NOT mean failure to conform to a specification but it means any potentially threatening system behavior. Some examples of critical system could be Communication systems, radio systems, command and control systems, etc. Table 2 shows an example of a list of satellite internet assets' critical systems that need to be protected for reliable performance

Table 2 – LEO satellite internet critical systems

Asset	Critical systems
Satellite vehicle	Power supply system [5]
	Attitude determination and control system (ADCS) [5]
	Propulsion system [5]
	Thermal control system [5]
	Tracking, telemetry and control subsystem (TT&C) [5]
	Radio communication systems
Satellite constellation	Radio communication systems
	Optical intersatellite link communication system
Infrastructure networking system	Data storage systems
	Packet routing and switching systems
	Data processing systems
	Network monitoring systems
	Network security systems
Mission operation center (MOC) [2]	Command and control systems
	Data processing and distributing system
Ground station terminal	RF communication system
	Optical communication system
Mobile ground terminal	Power supply systems
	RF communication systems
Satellite terminal	Position, navigation and timing system (PNT) [3]
	Communication system
	Data storage system
	Data processing system

The "*Orient*" step gives/provides an asset identification table, which includes the organization's scope of operation, the assets used to deploy satellite internet service and the critical systems that need to be protected. Then, the table is used in the "*Risk Assessment*" step to identify the attack surfaces, potential threats and their impact on the organization's business. Below, an example of asset identification table.

Scope	Assets	Critical systems
Space segment	Satellite vehicle	Communication system Sensor system Command and control system
Ground segment	Ground terminal	RF Communication system
	Mission operation center	Command and control system Satellite locating and Monitoring system Networking system Data processing system

Figure 3 - An example of asset identification table

RISK ASSESSMENT

Risk assessment is the process of identifying the attack surfaces existing in the critical systems defined in the "*Orient*" step. These attack surfaces are then used to identify the potential threats and their impact on national security or business operations if exploited by attackers or unauthorized individuals or entities. Risk assessment is a general concept that is commonly found in cyber security as well as the business field. Many techniques have been provided to conduct a risk assessment including some well-known risk management standards, e.g., the National Institute of Standards & Technology (NIST) "guide for conducting risk assessments" (NIST standard SP 800-30r1). It is worth revising the NIST standard SP 800-30r1 for better understanding.

Risk assessment is considered a critical activity, as it provides the foundation for the identified risks to be considered. Normally, it is guided by the organization's risk management process. The outcome of this activity is a comprehensive report that can support the risk management team in their decision making. By evaluating possible security threats and vulnerabilities over modules of the LEO satellite internet solution, then prioritizing them in order to define most impactful threats and less impactful ones. This outcome is mandatory for the next step "*Security Controls*" as it is used to create the organization's security profile and then filling the questioner to determine whether the organization applies the security requirements or not. This will be detailed in the following sections.

1- IDENTIFY ATTACK SURFACES AND POTENTIAL THREATS AND POSSIBLE IMPACT

Risk assessment starts by identifying the attack surfaces existing in each critical system that attackers can exploit. According to National Institute of Standards and Technology (NIST), attack surface is defined as the set of points on the boundary of a system, a component, or an environment where an attacker can gain access, or extract data [4], The smaller the attack surface, the harder for the attacker to compromise the system. Therefore, the attack surface should be minimized to reduce the risk of attack success.

The following table is adopted from open web application security project (OWASP) standard for internet of things security and updated to match the attack surface contained in the satellite internet critical systems. The table lists the attack surfaces that exists in most of LEO satellite internet critical systems and in different scope of operation along with potential threats and impacts on the system when any of these threats is conducted.

Table 3 - LEO satellite Internet attack surfaces, potintial threats and its impact

Attack Surface	Scope/critical systems	Potential threat	Possible Impact
Hardware and Sensors	Space segment [satellite vehicle] User segment [satellite terminal]	- Sensing Environment Manipulation. - Tampering (Physically). - Damage (Physically).	- Inject false reading. - Steal the device. - Update the firmware with malicious code and take control of the device.

Device Firmware	Space segment [satellite vehicle] User segment [satellite terminal]	- Sensitive data exposure (backdoor accounts, hardcoded credentials, encryption keys, sensitive information). - Firmware version display and/or last update date. - Firmware downgrade possibility.	- Access the secret keys, user credentials and organization credentials. - Unauthorized access to the Satellite system. - Access sensitive information about the firmware. - Create backdoor accounts through the firmware.
Device Memory	Space segment [satellite vehicle] User segment [satellite terminal]	- Sensitive data (Cleartext usernames, cleartext passwords, encryption keys that are used to authenticate to the satellite internet system).	- Access security keys. - Unauthorized access through stolen credentials. - Access data transmitted over between satellite and satellite terminal. - Ability to decrypt sensitive information and communication using stolen encryption keys.
Device Physical Interfaces	Space segment [satellite vehicle] User segment [satellite terminal]	- Firmware extraction. - Removal of storage media. - Tamper resistance. - Debug port (UART (Serial), JTAG / SWD)	- Get device ID. - Device malfunction. - Gain shell access to the OS using physical interfaces. - Modifying the source code control flow graph to do malicious activities.
Network Traffic	Ground segment [Core network] Space segment [satellite vehicle] User segment [satellite terminal]	- LAN - LAN to Internet - Non-standard - Wireless channels between segments - Protocol fuzzing	- Prevent the transmission of legitimate data. - Get sensitive data and information. - Analyze network traffic. - Privacy breach. - Integrity breach.
Update Mechanism	Space segment [satellite vehicle] User segment [satellite terminal]	- Update sent without encryption - Updates not signed - Update location writable - Update verification - Update authentication - Malicious update - Missing update mechanism	- Get a copy of the firmware. - Inject a rogue firmware update to the device resulting in getting access to sensitive information and modify the code control flow graph.
Device Network Services	Ground segment [Core network] Space segment [satellite vehicle] User segment [satellite terminal]	- Information disclosure - Administrative CLI - Injection - Denial of Service - Unencrypted Services - Poorly implemented encryption - Test/Development Services - Buffer Overflow - UPnP - Vulnerable UDP Services - DoS - Replay attack - Lack of payload verification	- Launch DoS, buffer overflow and replay attacks - Prevent the transmission of legitimate data. - Access sensitive data. - Analyze network traffic. - Privacy breach. - Integrity breach. - Access network security keys and decrypt the communications. - Grant unauthorized access to the network.

		- Lack of message integrity check - Credential management vulnerabilities (Username enumeration, Weak passwords, Account lockout, Known default credentials, Insecure password recovery mechanism).			
Authentication/ Authorization	Space segment [satellite vehicle] User segment [satellite terminal]	- Authentication/Authorization related values disclosure - Reusing of session key, token, etc. - Device to device authentication - Lack of dynamic authentication		- Gain unauthorized access to the system. - Take control of the system - Change system parameters and configuration. - Inject malicious data. - Unauthorized access to the system using a legit account.	
Local Data Storage	User segment [satellite terminal]	- Unencrypted data. - Data encrypted with discovered keys. - Lack of data integrity checks. - Use of static same enc/dec key.		- Discover secret credentials. - Access sensitive information. - Modify pre-stored information.	
Privacy	Ground segment Space segment [satellite vehicle] User segment	- User data disclosure - User/device location disclosure - Differential privacy		- Access user's personal information. - User and organization privacy breaches.	

In the following table, we derive the critical systems from assets defined in the asset identification in Figure 3. Then, the attack surfaces affecting these critical systems are identified and added to the table with the corresponding potential threats augmented by their impact (see Figure 4).

Assets	Critical systems	Attack surface	Potential threat	Impact
Satellite vehicle	Sensor system	Hardware and Sensors	- Sensing Environment Manipulation. - Tampering (Physically). - Damage (Physically).	- Inject false reading. - Steal the device. - Update the firmware with malicious code and take control of the device.
	Command and control system	Device Network Services	- Information disclosure - Unencrypted Services - Poorly implemented encryption	- Launch DoS, and replay attacks - Grant unauthorized access to the network.

Figure 4 – An example of potential threats and their impact

2- CLASSIFY THE THREATS IMPACT

The attack surface is then used to identify the threat class which is the area affected when the potential threat is conducted to the system. These threats could be classified into three classes:

1- National security threats
2- Network security threats
3- Equipment security threats

The threat class is used to categorize the potential threats and their impact, which in turn enables the service provider to deal with these threats in an organized manner based on class priority. Table 4 shows threat class categories and their potential threats.

Table 4 – Threat class categories and their potential threats

Threat class	Potential Threats
National security threats	**Threat** steal strategic information of target countries by deploying earth observation payload on LEO satellites. **Explanation** if the satellite internet constellations were equipped by high resolution cameras or any other equipment that could be used for picking earth images, this could lead to stealing strategic information and military locations imaging which causes a threat to national security. **Impact** Exposure of high confidentiality military and strategic location
Network security threats	**Threat** Identity Impersonation **Explanation** In such attacks, the attacker could disguise as any part of the system and communicate with other parts of the satellite system as if it is the legitimate associate, this could be done in three ways: o Attacker can disguise as a satellite terminal by calculating the uplink signal according to the downlink signal and use satellite equipment o Attacker can disguise as satellite network inducing the legal satellite terminal and user's end devices to access his network o Attacker can disguise as adjacent satellite in the same of different orbit inducing the target satellite network to establish ISL "inter-satellite link" with it to obtain relevant data transmitted between satellites. **Impact** Unauthorized access to the network service Exposure or user's IDs, information and location Exposure of network information
	Threat Data eavesdropping **Explanation** Because of the openness of the wireless communication there are three channels that can be eavesdropped user link [between satellite terminal and satellite], feed link [between satellite and the ground station] and ISL "inter-satellite link" [between 2

satellites]. Attackers can use receiving cards, retired satellite equipment or another satellite in LEO to receive the transmitted data and perform attacks,

Impact

Data leakage, insertion, modification

Threat

Information interception

Explanation

If the orbit of a foreign satellite is lower than that of a domestic satellite (for instance, the lowest orbit of SpaceX is about 300-500km), the attacker can perform the attack similar to the terrestrial pseudo base station to carry out network attacks to get user's information such as identification, and location.

Impact

Data and Information exposure

Threat

Signal interference

Explanation

by transmitting a high-powered signal into the same band as the target satellite, causing denial of service and preventing the satellite from receiving the signal properly. Signal interference can be done on both uplink and downlink signals by utilizing a ground station to broadcast signals on the same frequency to the satellite,

Impact

Satellite internet service disruption

Threat

Denial of service (DOS)

Explanation

DDoS attacks in satellite internet networks could be performed in the same manner that they are carried out on terrestrial networks. Attackers might employ software to initiate a large number of connection requests to the satellite, causing satellite failure to serve legitimate customers. Because of the limited number of satellite links in a satellite system, this attack is difficult to handle.

Impact

Satellite internet service disruption

Threat

	Anonymous attacking **Explanation** "Space is owned by global commons and has no national boundaries". So, it is possible for attackers to launch anonymous attacks against the target satellite in space. It is difficult for the attacked satellite to trace back the attack to the malicious actor due to the long distance and limited information. Not to mention that operations in the space environment can be disrupted by so many factors, so the problem could be caused by something other than a cyber-attack such as changes in the surrounding environment, design defects or device problems. This enables the attacker to deny their relation to the attack. Similarly, it is difficult for the ground station to accurately judge what is happening in space. **Impact** Denying of attacking responsibility
	Threat Malicious occupation of satellite bandwidth **Explanation** A satellite is a limited resource system "limited in power, memory, processing power and wireless resources" this makes satellite unsuitable for complex payload communication. So, to make it simple, most satellites use bent-pipe transponders which retransmit the received signal as it is, without processing or packet un-packing which will make it impossible to determine whether the data is from the legitimate user or not. Attackers can exploit that by sending data to the target satellite. Then building a receiving system to demodulate the downlink and get the data back elsewhere consuming satellite bandwidth. **Impact** Unauthorized usage of the systems resources
Equipment Security Threats	**Threat** Malicious satellite control **Explanation** By issuing malicious instructions or injecting malicious code to satellite nodes from ground facilities or space to achieve the goal of controlling satellites **Impact** Steal the satellite vehicle
	Threat Malicious consumption of satellite resources **Explanation**

		By issuing malicious instructions or injecting malware to consume power, processing time, bandwidth or memory
	Impact	Un stable operation of the satellite or device shutting off

The impact class classification is added to the table of potential threats (in Figure 4) to categorize each impact with the corresponding class as demonstrated in Figure 5.

Assets	Critical systems	Attack surface	Potential threat	Impact	Impact Class
Satellite vehicle	Sensor system	Hardware and Sensors	- Sensing Environment Manipulation. - Tampering (Physically). - Damage (Physically).	- Inject false reading. - Steal the device. - Update the firmware with malicious code and take control of the device.	Equipment Security Threats
	Command and control system	Device Network Services	- Information disclosure - Unencrypted Services - Poorly implemented encryption	- Launch DoS, and replay attacks - Grant unauthorized access to the network.	Network security threats

Figure 5 - An example of threat classification table

3- PRIORITIZE THREATS

After listing all the possible threats that could be applied to the system, prioritizing risks is an essential step to determine the mitigations needed based on threat level. In this context, the prioritization phase is carried out through two steps:

1- Prioritizing threats based on impact class [refer to Step 2: "*Classify the threats impacts*"]

2- Prioritizing threats based on risk matrix (the correlation between threat likelihood and the severity levels)

3.1. Prioritizing threats based on impact class

In this step, a prioritization level is determined according to the threats' impact. Table 5 demonstrates each security threat class and its corresponding impact level.

Table 5 – Impact level

Security Threat class	Impact level	Explanation
National security threats	National	These threats include compromising national strategic information security and military security threats that could lead to expose confidential content, images, information
Network security threats	Network	These threats are the threats that when exploited it leads to compromise the networking and intercept data which lead to leak of users' information or denial of service but have no effect on security of national or military entities
Equipment security threats	Equipment	These threats when being compromised it led to loss of one equipment (or causing it to stop operating normally) but has no major effect in the whole satellite system

3.2. Prioritizing threats based on risk matrix

In this step, a prioritization level is assigned to each threat according to its severity and likelihood. The risk assessment matrix is then used to map the risk level with both the severity and likelihood. Below an example of 5x5 risk assessment matrix.

			Severity Level				
			Very Low	Low	Moderate	High	Critical
			Negligible effect	Limited effect	Serious effect	Severe effect	Multiple severe effects
Likelihood	Critical	Almost certain	Very Low	Low	Moderate	High	Very High
	High	Highly likely	Very Low	Low	Moderate	High	Very High
	Moderate	Somewhat likely	Very Low	Low	Moderate	Moderate	High
	Low	Unlikely	Very Low	Low	Low	Low	Moderate
	Very Low	Highly unlikely	Very Low	Very Low	Very Low	Low	Low

Figure 6 – An example of 5x5 threat matrix

Then, the risk level will be utilized to prioritize the potential threats. Figure 7 shows the risk levels and their descriptions.

Risk level	Description
Very Low	Threat could be expected to have a negligible effect.
Low	Threat could be expected to have a limited effect.
Moderate	Threat could be expected to have a serious effect.
High	Threat could be expected to have a severe or catastrophic effect.
Critical	Threat could be expected to have multiple severe or catastrophic effects.

Figure 7 – The risk levels

3.3. Computing the risk level

Based on prioritization phase of potential threats (sub-section 3.1 and 3.2), a risk level is assigned for each threat. Figure 8 shows an example of a risk register table containing a list of potential threats and their corresponding impact, impact level, severity, likelihood and risk level.

Potential threat	Impact	Impact level	Severity	Likelihood	Risk level
Jamming military signals	Denial of service of military assets	National	Critical	Somewhat likely	High
Spoofing	Loss of satellite	Equipment	Critical	Almost certain	Very high
Hijacking and unauthorized commands to guidance control	Loss of satellite vehicle	Equipment	Critical	Highly likely	Very high
Denial-of-service attack	Loss of data and/or loss of service	Network	Moderate	Somewhat likely	Moderate

Figure 8 – An example of a risk register table

It should be noted that the risk register table will be used to classify the security control classes that should be implemented by the organization.

CYBER SECURITY CONTROLS

The security control is divided into two steps; first step is to match the security class controls. The constructed risk register is used to place each threat/vulnerability to one of the five NIST core areas. NIST core areas are functionalities that help in explaining the context of the categories and sub categories of cybersecurity controls.

- **Identify**
  - To identify the organization assets, business environment, risks and strategies that are used by the organization to enables the LEO satellite internet system
  - Identify potential threats and vulnerabilities that may affect these assets.
  - Model the threats
- **Protect**
  - Protect these assets by applying related controls and standards
  - Develop a strategy for awareness and training
- **Detect**
  - Perform regular vulnerability scanning
  - Add anomaly-based detection.
  - Continuously monitor the system to detect cyber security incidents
- **Response**
  - Perform actions to respond to those incidents
  - Develop a plan to improve the system after a cyber security incident
- **Recover**
  - Actions to recover the system back into its normal operation after incidents

Figure 9 – NIST core areas

For each risk level, a security class must be satisfied by the company/organization to comply the minimum-security requirements for each potential threat. Table 6 demonstrates the minimum-security functionalities required to be implemented for each security class.

Table 6 – Security class mapping with NIST core areas

		NIST Core areas				
Risk level	Security class	Identify	Protect	Detect	Respond	Recover
Very Low	Class 1	✓	✓	✗	✗	✗
Low	Class 2	✓	✓	✗	✗	✗
Moderate	Class 3	✓	✓	✗	✗	✓
High	Class 4	✓	✓	✓	✓	✓
Critical	Class 5	✓	✓	✓	✓	✓

For the "National" impact level, all the NIST core areas must be satisfied regardless the risk level or the security class of the threat

Potential threats	Class	Identify	Protect	Detect	Respond	Recover
Jamming and spoofing of sensor data	0	✓	✓	✗	✗	✗
Interception and theft of sensor data	0	✓	✓	✗	✗	✗
Hijacking and unauthorized commands to guidance control	4	✓	✓	✓	✓	✓
Denial of service attack	1	✓	✓	✗	✗	✓

Figure 10 – An example of security class table

The security class table is used to match the provided security controls with the appropriate mitigation techniques. In this context, a security profile is created to list the security controls that are currently implemented by the organization.

The organization should consider all the subcategories and controls outlined in the cybersecurity framework and select those that are currently in practice. This shall form the organization's profile table which should be used for filling the questionnaire with the appropriate response, evidence and reasons which will be explained in the next step. Figure 11 demonstrates an example of a security profile for an organization.

Function	ID	Subcategories
Identify	ID-1	Asset vulnerabilities are identified and documented.
	ID-3	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm that they are meeting their contractual obligations.
Protect	P-3	Access permissions and authorizations are managed to incorporate the principles of least privilege and separation of duties.
	P-6	Data-at-rest is protected.
	P-19	Protect satellite from Electromagnetic pulses
Detect	=	
	……	……
Respond		
	……	……
Recover		
	……	……

Figure 11 – A snapshot for an example of organizational risk profile

The following table lists the controls along with reference and control identification number, all classified into the NIST's five core areas for ease the selection of the appropriate controls as explained earlier in this step

Table 7 - List of LEO satellite internet controls categories

Function	ID	Control Category	Informative reference
Identify	ID-1	Asset vulnerabilities are identified and documented.	"NIST SP 800-53, REV. 5"
	ID-2	Cyber threat intelligence is received from information-sharing forums and sources.	
	ID-3	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm that they are meeting their contractual obligations.	
Protect	P-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	
	P-2	Remote access is managed.	
	P-3	Access permissions and authorizations are managed to incorporate the principles of least privilege and separation of duties.	
	P-4	Identities are proofed and bound to credentials and asserted in interactions.	
	P-5	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	
	P-6	Data-at-rest is protected.	
	P-7	Data-in-transit is protected.	
	P-8	An adequate capacity to ensure availability is maintained.	
	P-9	integrity-checking mechanisms are used to verify software, firmware, and information integrity.	
	P-10	Integrity-checking mechanisms are used to verify hardware integrity.	
	P-11	A baseline configuration of information technology/industrial control systems that incorporates security principles (e.g., concept of least functionality) is created and maintained.	
	P-12	Configuration change control processes are in place.	
	P-13	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	
	P-14	A vulnerability management plan is developed and implemented.	
	P-15	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	

	P-16	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	
	P-17	Communications and control networks are protected.	
	P-18	Mechanisms (e.g., fail safe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	
	P-19	Protect satellite from Electromagnetic pulses	
Detect	D-1	Event data are collected and correlated from multiple sources and sensors.	
	D-2	The network is monitored to detect potential cybersecurity events.	
	D-3	Malicious code is detected.	
	D-4	Monitoring for unauthorized personnel, connections, devices, and software is performed.	
	D-5	Event detection information is communicated.	
	D-6	Assets performance, locations are monitored (for satellite vehicle)	
Respond	RS-1	Voluntary information-sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.	
	RS-2	Notifications from detection systems are investigated.	
	RS-3	Forensics are performed.	
	RS-4	Incidents are contained.	
Recover	RC-1	The recovery plan is executed during or after a cybersecurity incident.	
	RC-2	Recovery strategies are updated.	

A detailed explanation and requirements are listed in Appendix B

CONFORMITY ASSESSMENT

Conformity assessment is the final step of the LEO satellite internet security assurance process, where conformity with the relevant security requirements is assessed with evidence. To do so, an LEO satellite internet security compliance assessment questionnaire checklist covering the key requirements-based questions is provided, as an audit and assessment tool. Every requirement under questioning is accompanied with its corresponding applicable NIST core area.

The organization shall fill/answer questions of requirements covering the applicable area matched with each category in risk profile [resulted in the previous step] to determine the conformity of the service provider organization, and the LEO satellite internet solution to the cybersecurity framework.

The organization shall answer all questions applicable on the determined security scope of the LEO satellite internet solution. It should provide supporting evidence and reasons for their answers wherever possible. The resulting checklist answers should clearly verify whether the LEO satellite internet service provider complies with the presented security baseline requirements or not. This compliance assessment questionnaire is intended to help organizations achieve high quality, informed security choices by guiding users through a robust checklist and evidence collecting process.

THE LEO SATELLITE INTERNET SECURITY COMPLIANCE ASSESSMENT QUESTIONNAIRE

The LEO satellite internet security compliance assessment questionnaire document is a part of the LEO satellite internet Security Guidelines Framework in the ARE. It provides a security assessment questionnaire checklist to guide LEO satellite internet service provider organizations through a security assessment process while collecting well-structured evidence and reasons, based on LEO satellite internet security best practices and requirements. After completing this checklist, organizations should be able to determine the compliance level of the LEO satellite internet solution.

Few foundations have provided security compliance questionnaires and checklists for the LEO satellite internet and cyber security in general. The LEO satellite internet security compliance assessment questionnaire provided with this framework follows applicable requirements from the NIST.SP.800-53r5, which is considered reliable and solid frameworks for relevant guidelines and standards. The LEO satellite internet security compliance assessment questionnaire can be found in Appendix C

It is also available in a separate document as an editable sheet for interested organizations, which should facilitate the process of completing the questionnaire by adding answers directly in the sheet. The editable sheet is attached to the framework and available upon request.

This assessment questionnaire is intended to help organizations achieve high quality, informed security choices by guiding them through a robust checklist and evidence collecting process.

THE USE OF ASSESSMENT QUESTIONNAIRE AND CHECKLIST SHEET

The process is guided by the category of the LEO satellite internet solution and the corresponding applicable scope of interest. Then the responses are captured on section 3 in the sheet. In order to use this checklist, the organization should first consider the LEO satellite internet Security assurance process described in section 3.

A risk assessment process should be first conducted in order to find applicable risks, that is used to create a current profile of the organization with respect to the organization’s scope of interest; For the

detailed process and extra demonstration, please refer to the LEO satellite Security assurance process (section 3).

COMPLETING THE CHECKLIST

The organization's representative members are responsible for filling/answering the checklist by providing a response, evidence, and a reason.

Response: Response is selected from four options described as shown in Table 8.

Table 8 - Checklist response options.

No	Mark	Response	Description
1	C	Compliant	The requirement is fully satisfied.
2	PC	Partially Compliant	The requirement is partially satisfied.
3	NC	Not Compliant	The requirement is not satisfied.
4	N/A	Not Applicable	The requirement is not applicable for the LEO satellite internet cybersecurity framework solution of concern.

Evidence: The response should be supported by an evidence document ensuring the provided response, wherever possible.
Reason: in case of not compliant and not applicable, a reason should be provided whenever needed to justify the provided response.

ASSESSMENT METHODOLOGY

After a service provider fills the questionnaire checklist document with the required input, an audit and review process is started by the NTRA to determine whether both the service provider organization and the provided technical service are compliant with the cybersecurity framework or not. After audition and review, the NTRA then provides a security compliance assessment report with the resulting compliance level decision, along with recommendations and suggestions.

REFERENCES

[1] Matthew Scholl; Theresa Suloway, "Introduction to Cybersecurity for Commercial Satellite Operations," NIST, U.S., 2022.

[2] Suzanne Lightman; Theresa Suloway; Joseph Brule, "Satellite Ground Segment," NIST, U.S., 2022.

[3] Michael Bartock; Joseph Brule; Ya-Shian Li-Baboud; Suzanne Lightman; James McCarthy; Karen Reczek; Doug Northrip; Arthur Scholz; Theresa Suloway , "Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services," NIST, U.S., 2021.

[4] MARFTIN, "The satellites subsystems," 14 Jul 2019. [Online]. Available: https://spaceradiation.eu/satellites-subsystems/?msclkid=482b4defc4a711ecbda0737b4d1ecf81.

[5] N. I. o. S. a. Technology, "Security and Privacy Controlsfor Information Systems and Organizations," NIST, U.S., 2020.

[6] "Low Earth orbit," [Online]. Available: https://en.wikipedia.org/wiki/Low_Earth_orbit.

[7] bell-labs, "telstart," [Online]. Available: https://www.bell-labs.com/about/history/innovation-stories/telstar-1/.

[8] "oneweb," [Online]. Available: https://oneweb.net/about-us/our-story.

[9] L. K. A. &. E. C. Vahid Joroughi, "5G Satellite Communications Services Through Constellation of LEO Satellites," *Springer*, 2019.

[10] M. Wall, "Arianespace launches 36 new OneWeb internet satellites into orbit on Soyuz rocket," 14 Oct 2021. [Online]. Available: https://www.space.com/arianespace-soyuz-rocket-oneweb-11-launch.

[11] V. Capitalist, "THE COST OF SPACE FLIGHT," 14 Fep 2022. [Online]. Available: https://www.newcapitalmgmt.com/news/the-cost-of-space-flight.

[12] T. Fernholz, "OneWeb is ready to challenge Elon Musk for satellite broadband dominance," Quartz, 2 Sep 2021. [Online].

[13] A. Jones, "China is developing plans for a 13,000-satellite megaconstellation," 21 Apr 2021. [Online]. Available: https://spacenews.com/china-is-developing-plans-for-a-13000-satellite-communications-megaconstellation/.

[14] B. Waidelich, "A Chinese Starlink? PRC Views on Building a Satellite Internet Megaconstellation," The Jamestown foundation, 22 Oct 2021. [Online]. Available: https://jamestown.org/program/a-chinese-starlink-prc-views-on-building-a-satellite-internet-megaconstellation/.

[15] W. Wang, "Near Optimal Timing and Frequency Offset Estimation for 5G Integrated LEO Satellite Communication System," Aug 2019.

[16] T. Fisher, "Tesla Phone," LifrWire, 30 Mar 2022. [Online]. Available: https://www.lifewire.com/tesla-phone-5212799.

[17] M. S. &. T. Suloway, "Introduction to Cybersecurity for Commercial Satellite Operations," National institute of standards and technology, U.S., 2022.

[18] "iFacts and Figures 2021: 2.9 billion people still offline," itu, 29 Nov 2021. [Online]. Available: https://www.itu.int/hub/2021/11/facts-and-figures-2021-2-9-billion-people-still-offline/.

[19] ITU, "Radio Regulations," 2016.

[20] "In-Space Propulsion Systems Roadmap," National Aeronautics and Space Administration, 2012.

[21] ARIANEGROUP, "CHEMICAL BI-PROPELLANT THRUSTER FAMILY," GERMANY.

[22] K. ZETTER, "Feds Say That Banned Researcher Commandeered a Plane," 15 May 2015.

[23] L. Shadbolt, "Technical Study Satellite Cyberattacks and security," Jul, 2021.

[24] H. C. &. L. Wu, "Analysis on the Security of Satellite Internet," in *CNCERT 2020. Communications in Computer and Information Science*, Singapore, 2020.

[25] T. Stremlau, "The vulnerability of satellite communications," security magazine, 19 Apr 2021. [Online]. Available: https://www.securitymagazine.com/articles/94689-the-vulnerability-of-satellite-communications.

[26] A. Spadafora, "Hacking satellite internet connections is a lot easier than you'd think," 12 Sep 2020. [Online]. Available: https://www.techradar.com/news/hacking-satellite-internet-connections-is-a-lot-easier-than-youd-think.

DOCUMENT HISTORY

Document history			
Edition	Date	Description	Unique ID
V0.1.0	April 2022	First release	ARE-LEO-SI-SEC-FW-010

APPENDIX A: CASE STUDY

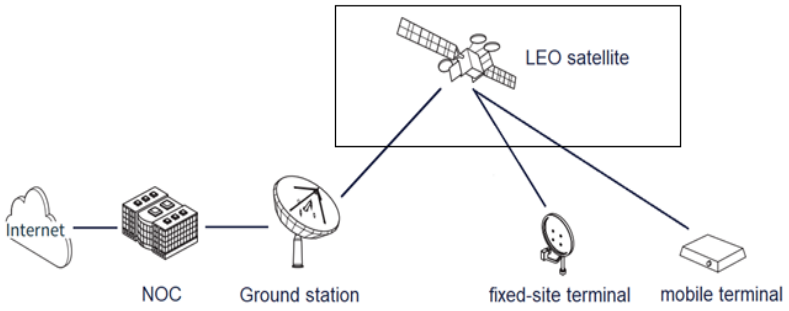
This section provides an example of how to use the framework to secure LEO satellite internet service and systems provided by a LEO satellite internet service provider, along with a step-by-step process for determining how compliant the company/organization is with the provided LEO satellite internet cyber security framework.

Consider a practical example of a LEO satellite internet service provider who offers an internet connectivity throughout LEO satellites to the customers. The service provider provides a satellite vehicle that allows to connect the user's devices (Satellite terminal) to ground station by sending/receiving data to/from the nearest LEO satellite. The following process explained in figure 1 is needed to comply with the framework.

The framework is aimed to address the NIST core areas and the applied cyber security controls to analyze the gap and fill in the questionnaire to perform conformity assessment which determines whether the company/organization compiles the minimum requirement of security to operate a LEO satellite internet system. NIST core areas are 5 functionalities that help to explain the context of the categories and subcategories of cybersecurity controls.

1. Orient

Organization starts by scoping the service/operations and set of systems it is interested in following the aspects of this following figure



For the company in this case of study, it owns the satellite vehicle and controls it. So according to the organization's scope all the following steps' outputs with be related to the scope of the company starting with critical systems and assets selection. Scope, assets and critical systems of satellite internet systems are listed in the following figure

Scope	Assets	Critical systems
Space segment	Satellite vehicle	Communication system Sensor system Command and control system

2. Risk Assessment

2.1. Identify attack surfaces and potential threats and the corresponding impact

The company performs risk assessment and vulnerability assessment to identify the attack surface and the potential threat as follows:

Assets	Critical systems	Attack surface	Potential threat	Impact
Satellite vehicle	Sensor system	Hardware and Sensors	- Sensing Environment Manipulation. - Tampering (Physically). Damage (Physically).	- Inject false reading. - Steal the device. Update the firmware with malicious code and take control of the device.

2.2. Classify the threat impacts

The identified threats could be classified as equipment security threats due to the fact that the affected area is limited to the satellite vehicle

Assets	Critical systems	Attack surface	Potential threat	Impact	Impact Class
Satellite vehicle	Sensor system	Hardware and Sensors	- Sensing Environment Manipulation. - Tampering (Physically). - Damage (Physically).	- Inject false reading. - Steal the device. - Update the firmware with malicious code and take control of the device.	Equipment Security Threats

2.3. Prioritize each threat

By classifying the identified threats, each threat is associated to a risk level, which will be used to classify the security class and determine the minimum NIST functionality to be implemented for mitigating such a threat.

Potential threat	Impact	Impact level	Severity	Likelihood	Risk level
Sensing Environment Manipulation.	Inject false reading.	Equipment	High	Moderate	Moderate
Tampering (Physically).	Steal the device.	Equipment	Critical	Very Low	Low
Damage (Physically).	Update the firmware with malicious code and take control of the device.	Equipment	Critical	Very Low	Low

3. Security Control

Each threat is classified to the appropriate class, which is used to determine the minimum functionality required to mitigate these threats.

Potential threats	Class	Identify	Protect	Detect	Respond	Recover
Sensing Environment Manipulation.	1	✅	✅	❌	❌	✅
Tampering (Physically).	0	✅	✅	❌	❌	❌
Damage (Physically).	0	✅	✅	❌	❌	❌

The class is then used to extract the security controls that applied by the company in for each threat and then use this to fill in the questionnaire. The output of this step is the organization's current security profile as demonstrated in the example figure below

Function	ID	Subcategories
identify	ID-1	Asset vulnerabilities are identified and documented.
	ID-3	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm that they are meeting their contractual obligations.
Protect	P-3	Access permissions and authorizations are managed to incorporate the principles of least privilege and separation of duties.
	P-6	Data-at-rest is protected.
	P-7	Data-in-transit is protected.
	P-10	Integrity-checking mechanisms are used to verify hardware integrity.
Recover	RC-1	The recovery plan is executed during or after a cybersecurity incident.
	RC-2	Recovery strategies are updated.

4. Conformity Assessment

This is the final step in the process where the service provider answers all the questionnaires which determines the conformity of the service provider organization, and the technical service to the cybersecurity framework. If the service provider, or the provided services are fully/partially compliant with the cybersecurity framework, evidence must be provided to support this claim. If the controls are not applicable to the service or the service is not compliant, a reason must be provided.

After the service provider fills the questionnaire document with the required input, the audit and review process from the NTRA starts to determine if both the service provider organization and the provided technical service are compliant with the cybersecurity framework.

TLP: AMBER

APPENDIX B: DETAILED SECURITY CONTROLS

The following table includes detailed overview for each category controls with each function having an abbreviation as following with the corresponding colour coding.

ID	Identify
P	Protect
D	Detect
RS	Response
RC	Recover

ID-1 Asset vulnerabilities are identified and documented.

Controls

ID-1-A Assessments

1- Select the appropriate assessor or assessment team for the type of assessment to be conducted
2- Develop a control assessment plan that describes the scope of the assessment including:
   a. Controls and control enhancements under assessment;
   b. Assessment procedures to be used to determine control effectiveness; and
   c. Assessment environment, assessment team, and assessment roles and responsibilities;
3- Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
4- Assess the controls in the system and its environment of operation [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;
5- Produce a control assessment report that document the results of the assessment; and
6- Provide the results of the control assessment to [*Assignment: organization-defined individuals or roles*]

ID-1-B Continuous monitoring

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

1- Establishing the following system-level metrics to be monitored: [Assignment: organization- defined system-level metrics];

2- Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;

3- Ongoing control assessments in accordance with the continuous monitoring strategy;

4- Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;

5- Correlation and analysis of information generated by control assessments and monitoring;

6- Response actions to address results of the analysis of control assessment and monitoring information; and

7- Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

ID-1-C Penetration Testing

Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].

ID-1-D Risk assessment

Conduct a risk assessment, including:

a. Identifying threats to and vulnerabilities in the system;

b. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and

c. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

1. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

2. Document risk assessment results in [Selection: security and privacy plans; risk assessment report; [Assignment: organization-defined document]];

3. Review risk assessment results [Assignment: organization-defined frequency];

4. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; and

5. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

ID-1-E Vulnerability monitoring and scanning

Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;

2. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for :

a. Enumerating platforms, software flaws, and improper configurations;

b. Formatting checklists and test procedures; and

c. Measuring vulnerability impact;

3. Analyse vulnerability scan reports and results from vulnerability monitoring;

4. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;

5. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and

6. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

ID-1-F System documentation

1. Obtain or develop administrator documentation for the system, system component, or system service that describes:

   a. Secure configuration, installation, and operation of the system, component, or service;
   b. Effective use and maintenance of security and privacy functions and mechanisms; and
   c. Known vulnerabilities regarding configuration and use of administrative or privileged functions.

2. Obtain or develop user documentation for the system, system component, or system service that describes:

   a. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms.
   b. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and
   c. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals.

3. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [*Assignment: organization-defined actions*] in response; and

4. Distribute documentation to [*Assignment: organization-defined personnel or roles*].

ID-1-G Developer testing and evaluation

Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:

1. Develop and implement a plan for ongoing security and privacy control assessments;
2. Perform [*Selection (one or more): unit; integration; system; regression*] testing/evaluation [*Assignment: organization-defined frequency*] at [*Assignment: organization-defined depth and coverage*];
3. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;
4. Implement a verifiable flaw remediation process; and
5. Correct flaws identified during testing and evaluation.

ID-1-H	Flow remediation

1. Identify, report, and correct system flaws;
2. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
3. Install security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and
4. Incorporate flaw remediation into the organizational configuration management process.

ID-1-I	System monitoring

1. Monitor the system to detect:

    a. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [*Assignment: organization-defined monitoring objectives*]; and

    b. Unauthorized local, network, and remote connections.

2. Identify unauthorized use of the system through the following techniques and methods: [*Assignment: organization-defined techniques and methods*];
3. Invoke internal monitoring capabilities or deploy monitoring devices:

    a. Strategically within the system to collect organization-determined essential information; and

    b. At ad hoc locations within the system to track specific types of transactions of interest to the organization.

4. Analyze detected events and anomalies;
5. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation.
6. Obtain legal opinion regarding system monitoring activities; and

Provide [*Assignment: organization-defined system monitoring information*] to [*Assignment: organization-defined personnel or roles*] [*Selection (one or more): as needed;* [*Assignment: organization-defined frequency*]].

ID-1-J	Security Alerts, Advisories and Directives

1. Receive system security alerts, advisories, and directives from [*Assignment: organization-defined external organizations*] on an ongoing basis;
2. Generate internal security alerts, advisories, and directives as deemed necessary;
3. Disseminate security alerts, advisories, and directives to: [*Selection (one or more):* [*Assignment: organization-defined personnel or roles*]; [*Assignment: organization-defined elements within the organization*]; [*Assignment: organization-defined external organizations*]]; and
4. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.

ID-1-K	Security and Privacy Groups and Associations
	Establish and institutionalize contact with selected groups and associations within the security and privacy communities: 1. To facilitate ongoing security and privacy education and training for organizational personnel; 2. To maintain currency with recommended security and privacy practices, techniques, and technologies; and

3. To share current security and privacy information, including threats, vulnerabilities, and incidents.

ID-2	Cyber threat intelligence is received from information-sharing forums and sources

Controls

ID-2-A Security Alerts, Advisories and Directives

Refer to ID-1-J

ID-2-C Security and Privacy Groups and Associations

Refer to ID-1-K

ID-2-D Threat awareness program

Implement a threat awareness program that includes a cross-organization information- sharing capability for threat intelligence.

ID-2-E Threat hunting

1. Establish and maintain a cyber threat hunting capability to:

    a. Search for indicators of compromise in organizational systems; and

    b. Detect, track, and disrupt threats that evade existing controls; and

2. Employ the threat hunting capability [*Assignment: organization-defined frequency*].

ID-3 Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm that they are meeting their contractual obligations

Controls

ID-3-A Audit record review, Analysis and Reporting

1. Review and analyze system audit records [*Assignment: organization-defined frequency*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*] and the potential impact of the inappropriate or unusual activity;
2. Report findings to [*Assignment: organization-defined personnel or roles*]; and
3. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

ID-3-B Control Assessments.

1. Select the appropriate assessor or assessment team for the type of assessment to be conducted;
2. Develop a control assessment plan that describes the scope of the assessment including:

    a. Controls and control enhancements under assessment;

    b. Assessment procedures to be used to determine control effectiveness; and

    c. Assessment environment, assessment team, and assessment roles and responsibilities;

3. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
4. Assess the controls in the system and its environment of operation [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;
5. Produce a control assessment report that document the results of the assessment; and
6. Provide the results of the control assessment to [*Assignment: organization-defined individuals or roles*].

ID-3-C Continuous monitoring

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

1. Establishing the following system-level metrics to be monitored: [*Assignment: organization- defined system-level metrics*];

2. Establishing [*Assignment: organization-defined frequencies*] for monitoring and [*Assignment: organization-defined frequencies*] for assessment of control effectiveness;

3. Ongoing control assessments in accordance with the continuous monitoring strategy;

4. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;

5. Correlation and analysis of information generated by control assessments and monitoring;

6. Response actions to address results of the analysis of control assessment and monitoring information; and

7. Reporting the security and privacy status of the system to [*Assignment: organization- defined personnel or roles*] [*Assignment: organization-defined frequency*].

ID-3-D	External personnel security

1. Establish personnel security requirements, including security roles and responsibilities for external providers;
2. Require external providers to comply with personnel security policies and procedures established by the organization;
3. Document personnel security requirements;
4. Require external providers to notify [*Assignment: organization-defined personnel or roles*] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [*Assignment: organization-defined time period*]; and
5. Monitor provider compliance with personnel security requirements.

ID-3-E	External system services

1. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [*Assignment: organization-defined controls*];
2. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and
3. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [*Assignment: organization-defined processes, methods, and techniques*].

ID-3-F	Developer testing and evaluation

Refer to ID-1-G

ID-3-G	Supply chain risk management strategy

1. Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;
2. Implement the supply chain risk management strategy consistently across the organization; and
3. Review and update the supply chain risk management strategy on [*Assignment: organization-defined frequency*] or as required, to address organizational changes.

P-1 Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes

Controls

P-1-A	**Identification And Authentication (non-organizational users)**
	Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

P-2 Remote access is managed

Controls

P-2-A	**Access control Policy and procedures**
	1. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: a. [Selection (one or more): Organization-level; Mission/business process-level; System- level] access control policy that: 1. (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and b. Procedures to facilitate the implementation of the access control policy and the associated access controls; 2. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and 3. Review and update the current access control: a. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and b. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
P-2-B	**Remote Access**
	1. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and 2. Authorize each type of remote access to the system prior to allowing such connections.
P-2-C	**Access control for mobile devices**
	1. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and 2. Authorize the connection of mobile devices to organizational systems.
P-2-D	**Collaborative computing devices and applications**

1. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]; and
2. Provide an explicit indication of use to users physically present at the devices.

P-3 Access permissions and authorizations are managed to incorporate the principles of least privilege and separation of duties

Controls

P-3-A Access Control Policy and procedures

Refer to P-2-A

P-3-B Account management

1. Define and document the types of accounts allowed and specifically prohibited for use within the system;
2. Assign account managers;
3. Require [*Assignment: organization-defined prerequisites and criteria*] for group and role membership;
4. Specify:

    a. Authorized users of the system;

    b. Group and role membership; and

    c. Access authorizations (i.e., privileges) and [*Assignment: organization-defined attributes (as required)*] for each account;

5. Require approvals by [*Assignment: organization-defined personnel or roles*] for requests to create accounts;
6. Create, enable, modify, disable, and remove accounts in accordance with [*Assignment: organization-defined policy, procedures, prerequisites, and criteria*];
7. Monitor the use of accounts;
8. Notify account managers and [*Assignment: organization-defined personnel or roles*] within:

    a. [*Assignment: organization-defined time period*] when accounts are no longer required;

    b. [*Assignment: organization-defined time period*] when users are terminated or transferred; and

    c. [*Assignment: organization-defined time period*] when system usage or need-to-know changes for an individual;

9. Authorize access to the system based on:

    a. A valid access authorization;

    b. Intended system usage; and

    c. [*Assignment: organization-defined attributes (as required)*];

10. Review accounts for compliance with account management requirements [*Assignment: organization-defined frequency*];

11. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
12. Align account management processes with personnel termination and transfer processes.

P-3-C	Access Enforcement

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies

P-3-D	Separation of Duties

1. Identify and document [*Assignment: organization-defined duties of individuals requiring separation*]; and
2. Define system access authorizations to support separation of duties

P-3-E	Least privilege

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

P-3-F	Concurrent Session Control

Limit the number of concurrent sessions for each [*Assignment: organization-defined account and/or account type*] to [*Assignment: organization-defined number*].

P-3-G	Security and Privacy Attributes

Provide the means to associate [*Assignment: organization-defined types of security and privacy attributes*] with [*Assignment: organization-defined security and privacy attribute values*] for information in storage, in process, and/or in transmission;

2. Ensure that the attribute associations are made and retained with the information;

3. Establish the following permitted security and privacy attributes from the attributes defined in G-1 just above for [*Assignment: organization-defined systems*]: [*Assignment: organization-defined security and privacy attributes*];

4. Determine the following permitted attribute values or ranges for each of the established attributes: [*Assignment: organization-defined attribute values or ranges for established attributes*];

5. Audit changes to attributes; and

6. Review [*Assignment: organization-defined security and privacy attributes*] for applicability [*Assignment: organization-defined frequency*].

P-3-H	Access Control Decisions

[*Selection: Establish procedures; Implement mechanisms*] to ensure [*Assignment: organization-defined access control decisions*] are applied to each access request prior to access enforcement.

P-4 Identities are proofed and bound to credentials and asserted in interactions.

Controls

P-4-A Security and Privacy Attributes

Refer to P-3-G

P-4-B Identification and Authentication (Policy and procedures)

1. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   a. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] identification and authentication policy that:

      1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      2. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   b. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;

2. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and
3. Review and update the current identification and authentication:

   a. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

b. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

P-4-C Identification and Authentication (Organizational Users)

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

P-4-D Identifier Management

Manage system identifiers by:

3. Receiving authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, service, or device identifier;
4. Selecting an identifier that identifies an individual, group, role, service, or device;
5. Assigning the identifier to the intended individual, group, role, service, or device; and
6. Preventing reuse of identifiers for [*Assignment: organization-defined time period*].

P-4-E Authenticator Management

1. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;
2. Establishing initial authenticator content for any authenticators issued by the organization;
3. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
5. Changing default authenticators prior to first use;

6. Changing or refreshing authenticators [*Assignment: organization-defined time period by authenticator type*] or when [*Assignment: organization-defined events*] occur;
7. Protecting authenticator content from unauthorized disclosure and modification;
8. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
9. Changing authenticators for group or role accounts when membership to those accounts changes.

P-4-F	Identity proofing

1. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;
2. Resolve user identities to a unique individual; and
3. Collect, validate, and verify identity evidence.

P-4-G	Physical Access authorizations

1. Screen individuals prior to authorizing access to the system; and
2. Rescreen individuals in accordance with [*Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening*].

P-5 Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).

Controls

P-5-A	Identification and Authentication (Policy and procedures)
	Refer to P-4-B
P-5-B	**Identification and Authentication (Organizational Users)**
	Refer to P-4-C
P-5-C	**Device Identification and Authentication**
	Uniquely identify and authenticate [*Assignment: organization-defined devices and/or types of devices*] before establishing a [*Selection (one or more): local; remote; network*] connection
P-5-D	**Authenticator Management**
	Refer to P-4-E
P-5-E	**Service Identification and Authentication**
	Uniquely identify and authenticate [*Assignment: organization-defined system services and applications*] before establishing communications with devices, users, or other services or applications
P-5-F	**Adaptive authentication**
	Require individuals accessing the system to employ [*Assignment: organization-defined supplemental authentication techniques or mechanisms*] under specific [*Assignment: organization-defined circumstances or situations*].
P-5-G	**Re-Authentication**
	Require users to re-authenticate when [*Assignment: organization-defined circumstances or situations requiring re-authentication*].

P-6 Data-at-rest is protected.

Controls

P-6-A	**Protection of Information at Rest**
	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].

POLICY

P-7 Data-in-transit is protected.

Controls

P-7-A	**Transmission Confidentiality and integrity**
	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information

P-8 An adequate capacity to ensure availability is maintained.

Controls

P-8-A	**Contingency plan**

1. Develop a contingency plan for the system that:

   a. Identifies essential mission and business functions and associated contingency requirements;

   b. Provides recovery objectives, restoration priorities, and metrics;

   c. Addresses contingency roles, responsibilities, assigned individuals with contact information;

   d. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;

   e. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;

   f. Addresses the sharing of contingency information; and

   g. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];

2. Distribute copies of the contingency plan to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*];

3. Coordinate contingency planning activities with incident handling activities;

4. Review the contingency plan for the system [*Assignment: organization-defined frequency*];
5. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
6. Communicate contingency plan changes to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*];
7. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and

Protect the contingency plan from unauthorized disclosure and modification.

P-8-B	Emergency power

Provide an uninterruptible power supply to facilitate [*Selection (one or more): an orderly shutdown of the system; transition of the system to long-term alternate power*] in the event of a primary power source loss

P-8-C	Denial of Service Protection

1. [*Selection: Protect against; Limit*] the effects of the following types of denial-of-service events: [*Assignment: organization-defined types of denial-of-service events*]; and
2. Employ the following controls to achieve the denial-of-service objective: [*Assignment: organization-defined controls by type of denial-of-service event*].

P-9 integrity-checking mechanisms are used to verify software, firmware, and information integrity.

Controls

P-9-A	Software, Firmware and Information Integrity

1. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [*Assignment: organization-defined software, firmware, and information*]; and
2. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [*Assignment: organization-defined actions*].

P-9-B	Information Input Validation

Check the validity of the following information inputs: [*Assignment: organization- defined information inputs to the system*].

P-9-C	Customized development of critical components

Reimplement or custom develop the following critical system components: [*Assignment: organization-defined critical system components*].

P-10 Integrity-checking mechanisms are used to verify hardware integrity.

Controls

P-10-A	**Software, Firmware and Information Integrity**
	Refer to P-9-A
P-10-B	**Customized development of critical components**
	Refer to P-9-C

P-11 A baseline configuration of information technology/industrial control systems that incorporates security principles (e.g., concept of least functionality) is created and maintained

Controls

P-11-A Baseline Configuration

1. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and
2. Review and update the baseline configuration of the system:

   a. [*Assignment: organization-defined frequency*];

   b. When required due to [*Assignment: organization-defined circumstances*]; and

   c. When system components are installed or upgraded.

P-11-B Configuration Change Control

Determine and document the types of changes to the system that are configuration- controlled;

2. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;

3. Document configuration change decisions associated with the system;

4. Implement approved configuration-controlled changes to the system;

5. Retain records of configuration-controlled changes to the system for [*Assignment: organization-defined time period*];
6. Monitor and review activities associated with configuration-controlled changes to the system; and
7. Coordinate and provide oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element*] that convenes [*Selection (one or more):* [*Assignment: organization-defined frequency*]; when [*Assignment: organization-defined configuration change conditions*]].

P-11-C Impact analysis

Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

P-11-D Access restrictions for change

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

P-11-E	Configuration settings

1. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [*Assignment: organization-defined common secure configurations*];
2. Implement the configuration settings;
3. Identify, document, and approve any deviations from established configuration settings for [*Assignment: organization-defined system components*] based on [*Assignment: organization-defined operational requirements*]; and
4. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

P-11-F	Least Functionality

1. Configure the system to provide only [*Assignment: organization-defined mission essential capabilities*]; and

2. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [*Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services*].

P-11-G	Configuration Management Plan

Develop, document, and implement a configuration management plan for the system that:

1. Addresses roles, responsibilities, and configuration management processes and procedures;
2. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
3. Defines the configuration items for the system and places the configuration items under configuration management;
4. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*]; and
5. Protects the configuration management plan from unauthorized disclosure and modification.

P-11-H	Developer Configuration Management

Require the developer of the system, system component, or system service to:

1. Perform configuration management during system, component, or service [*Selection (one or more): design; development; implementation; operation; disposal*];

2. Document, manage, and control the integrity of changes to [*Assignment: organization- defined configuration items under configuration management*];

3. Implement only organization-approved changes to the system, component, or service;

4. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and

5. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].

P-13 Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

Controls

P-13-A Least Functionality

Refer to P-11-F

P-14 A vulnerability management plan is developed and implemented

Controls

P-14-A Risk Assessment Policy and Procedures

1. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   a. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] risk assessment policy that:

      1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      2. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   b. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;

2. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and
3. Review and update the current risk assessment:

   a. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   b. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

P-14-B Risk Assessment

Refer to ID-1-D

P-14-C Vulnerability Monitoring and Scanning

Refer to ID-1-E

P-14-D Flow remediation

Refer to ID-1-H

P-15 Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.

Controls

P-15-A Audit and accountability (Policy and Procedures)

1. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   a. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] audit and accountability policy that:

      1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      2. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   b. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;

2. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and
3. Review and update the current audit and accountability:

   a. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   b. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

P-15-B Event Logging

1. Identify the types of events that the system is capable of logging in support of the audit function: [*Assignment: organization-defined event types that the system is capable of logging*];
2. Coordinate the event logging function with other organizational entities requiring audit- related information to guide and inform the selection criteria for events to be logged;
3. Specify the following event types for logging within the system: [*Assignment: organization-defined event types (subset of the event types defined in P-15-B point 1 above.) along with the frequency of (or situation requiring) logging for each identified event type*];
4. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
5. Review and update the event types selected for logging [*Assignment: organization-defined frequency*].

P-15-C Content of Audit Records

Ensure that audit records contain information that establishes the following:

1. What type of event occurred;
2. When the event occurred;
3. Where the event occurred;
4. Source of the event;
5. Outcome of the event; and
6. Identity of any individuals, subjects, or objects/entities associated with the event.

P-15-D Audit Record Review, Analysis and Reporting

1. Review and analyze system audit records [*Assignment: organization-defined frequency*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*] and the potential impact of the inappropriate or unusual activity;
2. Report findings to [*Assignment: organization-defined personnel or roles*]; and

3. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

P-15-E Audit Record Reduction and Report Generation

Provide and implement an audit record reduction and report generation capability that:

1. Supports on-demand audit record review, analysis, and reporting requirements and after- the-fact investigations of incidents; and

Does not alter the original content or time ordering of audit records

P-15-F Audit Record Generation

1. Provide audit record generation capability for the event types the system is capable of auditing as defined in B-1 (right above) on [*Assignment: organization-defined system components*];
2. Allow [*Assignment: organization-defined personnel or roles*] to select the event types that are to be logged by specific components of the system; and
3. Generate audit records for the event types defined in B-3 that include the audit record content defined in C.

P-15-G Monitoring for Information Disclosure

1. Monitor [*Assignment: organization-defined open-source information and/or information sites*] [*Assignment: organization-defined frequency*] for evidence of unauthorized disclosure of organizational information; and
2. If an information disclosure is discovered:

    a. Notify [*Assignment: organization-defined personnel or roles*]; and

    b. Take the following additional actions: [*Assignment: organization-defined additional actions*].

P-15-H Session Audit

1. Provide and implement the capability for [*Assignment: organization-defined users or roles*] to [*Selection (one or more): record; view; hear; log*] the content of a user session under [*Assignment: organization-defined circumstances*]; and
2. Develop, integrate, and use session auditing activities in consultation with legal counsel and in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

P-15-I Cross Organizational Audit Logging

Employ [*Assignment: organization-defined methods*] for coordinating [*Assignment: organization-defined audit information*] among external organizations when audit information is transmitted across organizational boundaries.

P-16 The principle of least functionality is incorporated by configuring systems to provide only essential capabilities

Controls

P-16-A Access Enforcement

Refer to P-3-C

P-16-B Least Functionality

Refer to P-11-F

P-17 Communications and control networks are protected.

Controls

P-17-A Session Termination

Automatically terminate a user session after [*Assignment: organization-defined conditions or trigger events requiring session disconnect*].

P-17-B Remote Access

Refer to P-2-B

P-17-C Telecommunications Services

Establish alternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

P-17-D Denial of Service Protection

Refer to P-8-C

P-17-E Boundary Protection

1. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
2. Implement subnetworks for publicly accessible system components that are [*Selection: physically; logically*] separated from internal organizational networks; and

Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture

P-17-F Network Disconnect

Terminate the network connection associated with a communications session at the end of the session or after [*Assignment: organization-defined time period*] of inactivity.

P-17-G Secure Name/Address Resolution Service (Authoritative Source)

1. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
2. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

P-17-H Architecture and Provisioning for Name/Address Resolution Service

Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

P-17-I	Session Authenticity

Protect the authenticity of communications sessions

P-17-J	Covert Channel Analysis

1. Perform a covert channel analysis to identify those aspects of communications within the system that are potential avenues for covert [*Selection (one or more): storage; timing*] channels; and
2. Estimate the maximum bandwidth of those channels.

P-17-K	Out of Band Channels

Employ the following out-of-band channels for the physical delivery or electronic transmission of [*Assignment: organization-defined information, system components, or devices*] to [*Assignment: organization-defined individuals or systems*]: [*Assignment: organization-defined out-of-band channels*].

P-17-L	Operations Security

Employ the following operations security controls to protect key organizational information throughout the system development life cycle: [*Assignment: organization-defined operations security controls*].

P-17-M	Alternate Communications Paths

Establish [*Assignment: organization-defined alternate communications paths*] for system operations organizational command and control.

P-18 Mechanisms (e.g., fail safe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

Controls

P-18-A	Emergency power

Refer to P-8-B

P-18-B	Security and Privacy Architectures

1. Develop security and privacy architectures for the system that:

    a. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;

    b. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;

    c. Describe how the architectures are integrated into and support the enterprise architecture; and

    d. Describe any assumptions about, and dependencies on, external systems and services;

2. Review and update the architectures [*Assignment: organization-defined frequency*] to reflect changes in the enterprise architecture; and
3. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

P-18-C	Resource Availability
	Protect the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more): priority; quota; [Assignment: organization-defined controls]].

P-19 Protect satellite from Electromagnetic pulses

Controls

P-19-A	Electromagnetic pulse protection
	Employ [Assignment: organization-defined protective measures] against electromagnetic pulse damage for [Assignment: organization-defined systems and system components].

D-1 Event data are collected and correlated from multiple sources and sensors.

Controls

D-1-A	Audit record review, Analysis and Reporting
	Refer to ID-3-A
D-1-B	**Continuous monitoring**
	Refer to ID-1-B
D-1-C	**Incident Handling**
	1. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery; 2. Coordinate incident handling activities with contingency planning activities; 3. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and 4. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.
D-1-D	**Incident Monitoring**
	Track and document incidents
D-1-E	**Incident Response Plan**
	. Develop an incident response plan that: a. Provides the organization with a roadmap for implementing its incident response capability; b. Describes the structure and organization of the incident response capability; c. Provides a high-level approach for how the incident response capability fits into the overall organization; d. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; e. Defines reportable incidents; f. Provides metrics for measuring the incident response capability within the organization;

g. Defines the resources and management support needed to effectively maintain and mature an incident response capability;

h. Addresses the sharing of incident information;

i. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*] [*Assignment: organization-defined frequency*]; and

j. Explicitly designates responsibility for incident response to [*Assignment :organization- defined entities, personnel, or roles*].

2. Distribute copies of the incident response plan to [*Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements*];

3. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

4. Communicate incident response plan changes to [*Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements*]; and

5. Protect the incident response plan from unauthorized disclosure and modification.

D-1-F **System monitoring**

Refer to ID-1-i

D-2 The network is monitored to detect potential cybersecurity events

Controls

D-2-A **Audit Record Generation**

1. Provide audit record generation capability for the event types the system is capable of auditing; [Assignment: organization-defined system components];

2. 2. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and

3. Generate audit records for the event types defined [Assignment: organization- defined event types]

D-2-B **Continuous monitoring**

Refer to ID-1-B

D-2-C **Configuration Change Control**

Refer to P-11-B

D-2-D **Denial of Service Protection**

Refer to P-8-C

D-2-E **Boundary Protection**

Refer to P-17-E

D-2-F	**System monitoring**
	Refer to ID-1-i

D-3 Malicious code is detected

Controls

D-3-A	**System monitoring**
	Refer to ID-1-i

D-4 Monitoring for unauthorized personnel, connections, devices, and software is performed

Controls

D-4-A	**Audit Record Generation**
	1. Provide audit record generation capability for the event types the system is capable of auditing; [Assignment: organization-defined system components]; 2. 2. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and 3. Generate audit records for the event types defined [Assignment: organization- defined event types]
D-4-B	**Continuous monitoring**
	Refer to ID-1-B
D-4-C	**Configuration Change Control**
	Refer to P-11-B
D-4-D	**System Component Inventory**
	1. Develop and document an inventory of system components that: a. Accurately reflects the system; b. Includes all components within the system; c. Does not include duplicate accounting of components or components assigned to any other system; d. Is at the level of granularity deemed necessary for tracking and reporting; and e. Includes the following information to achieve system component accountability: [*Assignment: organization-defined information deemed necessary to achieve effective system component accountability*]; and 2. Review and update the system component inventory [*Assignment: organization-defined frequency*].

D-4-E	**System monitoring**
	Refer to ID-1-i

D-5 Event detection information is communicated

Controls

D-5-A	**Audit record review, Analysis and Reporting**
	Refer to ID-3-A
D-5-B	**Assessments**
	Refer to ID-1-A
D-5-C	**Continuous monitoring**
	Refer to ID-1-B
D-5-D	**Vulnerability monitoring and scanning**
	Refer to ID-1-E
D-5-E	**System monitoring**
	Refer to ID-1-i

D-6 Assets performance and location are monitored (for satellite vehicle)

Controls

D-6-A	**Asset Monitoring And Tracking**
	Employ [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas].

RS-1 Voluntary information-sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.

Controls

RS-1-A	**Security Alerts, Advisories and Directives**
	Refer to ID-1-J
RS-1-B	**Security and Privacy Groups and Associations**
	Refer to ID-1-K

RS-2 Notifications and feeds from detection systems are investigated

Controls

RS-2-A	**Audit record review, Analysis and Reporting**
	Refer to ID-3-A
RS-2-B	**Continuous monitoring**
	Refer to ID-1-B
RS-2-C	**Incident Handling**
	Refer to D-1-C

RS-2-D	**Incident Monitoring**
	Track and document incidents
RS-2-E	**Monitoring Physical Access**
	1. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents; 2. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and 3. Coordinate results of reviews and investigations with the organizational incident response capability.
RS-2-F	**Vulnerability monitoring and scanning**
	Refer to ID-1-E
RS-2-G	**System monitoring**
	Refer to ID-1-i

RS-3 Audit Record Reduction and Report Generation

Controls

RS-3-A	**Audit record review, Analysis and Reporting**
	Provide and implement an audit record reduction and report generation capability that: 1. Supports on-demand audit record review, analysis, and reporting requirements and after- the-fact investigations of incidents; and 2. Does not alter the original content or time ordering of audit records
RS-3-B	**Incident Handling**
	Refer to D-1-C

RS-4 Incidents are contained

Controls

RS-4-A	**Incident Handling**
	Refer to D-1-C
RS-4-B	**Contingency plan**
	Refer to P-8-A
RS-4-C	**Incident Response Plan**
	Refer to D-1-E

RC-1 The recovery plan is executed during or after a cybersecurity incident.

Controls	
RC-1-A	**System Recovery and Reconstruction**
	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.
RC-1-B	**Incident Handling**
	Refer to D-1-C
RC-1-C	**Incident Response Plan**
	Refer to D-1-E

RC-2 Regular review and update of Recovery strategies.

Controls	
RC-2-A	**Contingency plan**
	Refer to P-8-A
RC-2-B	**Incident Handling**
	Refer to D-1-C
RC-2-C	**Incident Response Plan**
	Refer to D-1-E

APPENDIX C: LEO-SI SECURITY COMPLIANCE ASSESSMENT QUESTIONNAIRE CHECKLIST

PLEASE REFER TO THE ATTACHED DOCUMENT