#### 4.4 Respond Function

Develop and implement the appropriate activities to respond to a detected cybersecurity or anomalous event. The activities in the Respond Function support the ability to contain the impacts of an anomaly or attack.

The Respond Function serves as a list of recommended actions and is triggered by the outputs generated by the Detect Function. The Protect Function provides the ability for the Respond Function to execute the proper response to an event according to a predefined plan.

The objectives of the Response Function are to:

* Contain events using a verified response procedure.
* Communicate the occurrence and impact of the event on satellite operations and stakeholders.
* Develop processes to respond to and mitigate new known or anticipated threats or vulnerabilities; and
* Evolve response strategies and plans based on lessons learned.

The Respond Function within the Cybersecurity Framework defines five Categories, all of which applies to the SOC.

##### 4.4.1 Response Planning Category

Response processes and procedures are executed and maintained after detected cybersecurity incidents.

There is one subcategory within Response Planning.

# Table 17 - Response Planning Subcategory

|  |  |  |
| --- | --- | --- |
| **Respond: Response Planning**  **Subcategory**  **Applicability to SOC** | | **References** |
| **RS.RP-1: Response plan is executed during or after an incident.** | Execute the response plan during or after a cybersecurity event that impact space systems in accordance with the predefined threshold.  Document the steps and results of the response plans as they are being executed. Include categories of incidents resilience level requirements based on criticality and impact.  Update the response plans to address changes to the organization. | **NIST SP 800-53 Rev. 5** CP-2, CP-10, IR-4, IR-8 |

##### 4.4.2 Communications Category

Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies). In the context of the SOC, external stakeholders may include organizations that control third party hosts.

There are four Subcategories within the Communications Category that apply to the SOC, as summarized in the table below.

# Table 18 - Communications

|  |  |  |
| --- | --- | --- |
| **Respond: Communications**  **Subcategory**  **Applicability to SOC** | | **References** |
| **RS.CO-1: Personnel know their roles and order of operations when a response is needed** | Ensure that personnel know, are trained and have exercised their roles in response to disruptions.  Responders should understand recovery time objectives (RTO), recovery point objectives (RPO), restoration priorities, task sequences, and assignment responsibilities for event response programs and processes in a manner that is consistent with business continuity objectives. | **NIST SP 800-34 Rev.1** 3.2.1, CP-2, CP-3, IR-3, IR-8  **NIST SP 800-53 Rev. 5** CP-2, CP-3, IR-3,  IR-8  **NIST SP 800-61** |
| **RS.CO-2: Incidents are reported consistent with established criteria** | Ensure that cybersecurity events that exceed a predetermined threshold are reported in a manner that is consistent with the response plan and will initiate the response plan in a timely manner. | **NAVCEN**  **NIST SP 800-53 Rev. 5** AU-6, IR-6, IR-8  **NIST SP 800-61 Rev. 2 4**  **NERC CIP-008-6** |
| **RS.CO-3: Information is shared consistent with response plans** | Not applicable to the SOC. Satellites are a niche cyber operations and typically use specialized applications. | **FCC**  **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8  **NIST SP 800-61 Rev. 2** 2.4 |
| **RS.CO-4: Coordination with stakeholders occurs consistent with response plans** | In the event of a satellite that hosts third party payloads, incidents that impact satellite bus operations are reported to the stakeholders in accordance with the response plan and pre-arranged agreements with the payload stakeholders. | **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8, PE-6  **NIST SP 800-61 Rev. 2** 2.4 |
| **RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness** | Suspected intentional interference should be reported to stakeholders through the appropriate channels and procedures. For example, suspected land-based RFI can be reported to NAVCEN, NASA Aviation Safety Reporting System for aeronautics, or NERC E-ISAC for the electric utility sector.  When agreed upon between stakeholders, common data formats facilitate information sharing to strengthen the protection of the user community | **NIST SP 800-53 Rev.** 5, SI-5, PM-15 |

##### 4.4.3 Analysis Category

Analysis is conducted to verify effective response and support recovery activities. There are five Subcategories within the Analysis Category.

|  |  |  |
| --- | --- | --- |
| **Respond: Analysis**  **Subcategory**  **Applicability to the SOC** | | **References** |
| **RS.AN-1: Notifications from detection systems are investigated** | Investigate cybersecurity-related notifications generated from the anomaly detection systems.  Identify and locate potential sources of RFI. Upon determining that the source of an data anomaly is an RFI external to the organization’s system, partner with the appropriate external stakeholders for further investigation. DHS coordinates the development, implementation, and exercise of procedures to enable federal agencies with assigned responsibilities, authorities, and jurisdictions to investigate and mitigate satellite interference. Should multiple sensors report data anomaly events, analytics can be used to determine if the events are correlated or otherwise traced to a common causal agent | **NIST SP 800-53 Rev. 5** AU-6, CA-7, IR-4, IR-5, PE-6, RA-5, SI-4  **RTCA 235** 14.1.2 |
| **RS.AN-2: The impact of the incident is understood** | Within the SOC, understand the full implication of a cybersecurity incident based on thorough investigation and analysis results.  Consider downstream impacts and relationships through leveraging mapped services and outlined policies. Understand the impacts that may affect the space segment and third party stakeholders (in the case of SOCs that host third party payloads). | **NIST SP 800-53 Rev. 5** CP-2, IR-4, RA-3  **NIST SP 800-61 Rev. 2** 3 |
| **RS.AN-3: Forensics are performed** | Conduct forensic analysis on collected cybersecurity event information to determine if there are any residual effects to the system.  Conduct forensic analysis to aid in the determination of the root cause. | **NIST SP 800-53 Rev. 5** AU-7, IR-4  **NIST SP 800-61 Rev. 2** 3 |
| **RS.AN-4: Incidents are categorized consistent with response plans** | Categorize cybersecurity incidents according to the level of severity and impact consistent with the response plan. | **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-5, IR-8, RA-3  **NIST SP 800-61 Rev. 2** 2 3.2 |
| **RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)** | With the exception of RFI reporting, not applicable to the SOC. | **GPS-ICD-240** 7.6, 7.7  **NCCIC**  **NIST SP 800-53 Rev. 5** CA-1, CA-2, PM-4, PM-15, RA-1, RA-7, SI-5, SR-6  **NIST SP 800-61 Rev. 2** 3, 3.2  **NIST SP 800-160 Rev. 1** 3.4.9, 3.4.11 |

##### 4.4.4 Mitigation Category

Activities are performed to contain an event, mitigate its effects, and resolve the incident. There are three Subcategories within the Mitigation Category.

# Table 20 - Mitigation Subcategories

|  |  |  |
| --- | --- | --- |
| **Respond: Mitigation**  **Subcategory**  **Applicability to SOC** | | **References** |
| **RS.MI-1: Incidents are contained** | Contain cybersecurity incidents to minimize impacts on the SOC. Containment may require the transition to the alternate SOC and isolation of the primary SOC in accordance with resiliency level requirements and the business continuity plan for containment. | **NIST SP 800-53 Rev. 5** IR-4  **NIST SP 800-61 Rev. 2** 3.4.1 |
| **RS.MI-2: Incidents are mitigated** | Once the effects of the incident are contained, take steps to return the SOC to a proper working state. These steps may include the resetting, recalibration, and replacement of units in a manner that does not impact forensic efforts.  Apply patches and updates to mitigate the vulnerability.  Consider mitigation strategies such as redundancy, diversity, and segmentation to minimize the impacts of SOC disruption. | **NIST SP 800-53 Rev. 5** IR-4  **NIST SP 800-61 Rev. 2** 3.4 |
| **RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks** | Risk assessments (refer to Identify: Risk Assessment category) should be updated with newly identified vulnerabilities and mitigated or documented as acceptable risks.  Maintain an RFI incident database in order to inform future detection, protection and mitigation strategies. | **NIST SP 800-53 Rev. 5** CA-2, CA-7, RA-3, RA-5, RA-5  **NIST SP 800-61 Rev. 2** 3  **RTCA 235** 14.1.4, 14.2-14.4, 3.8 |

##### 4.4.5 Improvements Category

This category is a post incident analysis activity that involves other functions within the CSF. Organizational response activities are improved by incorporating lessons learned from current and previous detection and response activities. Both Subcategories within the Improvements Category apply to the SOC.

# Table 21 - Improvements Subcategories

|  |  |  |
| --- | --- | --- |
| **Respond: Improvements**  **Subcategory**  **Applicability to SOC** | | **References** |
| **RS.IM-1: Response plans incorporate lessons learned** | Response plans incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing and implement the resulting changes accordingly. | **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8  **NIST SP-800-61 Rev. 2** |
| **RS.IM-2: Response strategies are updated** | Enable an update process for the response plan to consider new threats, improved technology, and lessons learned.  Analyze detected event information and incident responses to reassess the impact of future incidents to the organization. If appropriate, update the risk assessment and risk response.  Determine preventative actions for fault modes by reviewing the identification, protection, and detection functions and updating as applicable.  Revise protection, monitoring, detection, response, and recovery capabilities as needed to mitigate newly identified vulnerabilities in a timely manner. | **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8 |

#### 4.5 Recover Function

The Recover Function develops and implements the appropriate activities to maintain resilience and restore any capabilities or services that were impaired due to a cybersecurity event.

The activities in the Recover Function support timely recovery to normal operations and return the organization back to its proper working state after an incident has occurred. The effectiveness of the Recover Function is dependent upon the implementation of the previous Functions—Identify, Protect, Detect, and Respond.

The objectives of the Recovery Function are to:

* Restore systems dependent upon the SOC services to a proper working state using a verified recovery procedure.
* Communicate the recovery activities and status of the SOC services to stakeholders; and
* Evolve recovery strategies and plans based on lessons learned.

The Recover Function within the Cybersecurity Framework defines three Categories.

##### 4.5.1 Recovery Planning Category

Recovery processes and procedures are executed and maintained to restore systems or assets affected by cybersecurity incidents to a proper working state.

There is one Subcategory within Recovery Planning that applies to the SOC.

# Table 22 - Recovery Planning Subcategory

|  |  |  |
| --- | --- | --- |
| **Recover** : **Recovery Planning**  **Subcategory**  **Applicability to the SOC** | | **References** |
| **RC.RP-1: Recovery plan is executed during or after a cybersecurity incident.** | A recovery plan is typically a part of the business continuity plan.  Restore the SOC system within a predefined, acceptable time period from configuration-controlled and integrity protected information representing a known good state for the components.  Perform system acceptance testing.  The recovery plan can include specific actions for restoration, recalibration, resetting, and test validation of equipment. | **NIST SP 800-34 Rev. 1**  **NIST SP 800-53 Rev. 5** CP-10, IR-4, IR-8  **NIST SP 800-160 Rev. 1** 3.4.11, Appendix F.2.6  **NIST SP 800-184** |

##### 4.5.2 Improvements Category

Recovery planning and processes are improved by incorporating lessons learned into future activities. In the context of the SOC, the efficacy of the recovery actions, such as restoring control of the space segment, test plans, user notification and failover, are evaluated and improved should a similar event occur.

There are two Subcategories within the Improvements Category.

# Table 23 - Improvements Subcategories

|  |  |  |
| --- | --- | --- |
| **Recover** : **Improvements**  **Subcategory**  **Applicability to the SOC** | | **References** |
| **RC.IM-1: Recovery plans incorporate lessons learned.** | A recovery plan is typically a part of the business continuity plan.  Restore the SOC system within a predefined, acceptable time period from configuration-controlled and integrity protected information representing a known good state for the components.  Perform system acceptance testing.  The recovery plan can include specific actions for restoration, recalibration, resetting, and test validation of equipment. | **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8  **NIST SP 800-61 Rev. 2** 3.4 |
| **RC.IM-2: Recovery strategies are updated.** | Update the recovery plan to incorporate lessons learned, reflect new threats, improve technology, and address changes to the organization, operating environment, and deficiencies encountered during plan implementation, execution, and testing.  Recovery timeliness and prioritization based on application criticality are key to reducing impacts. Evaluate incident characteristics to determine the optimal recovery strategy and revise the recovery plan as needed. | **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8 **NIST SP 800-61 Rev. 2** 3.4,3.4.1 |

##### 4.5.3 Communications Category

Restoration activities are coordinated with internal and external parties. In the context of the SOC, external parties may include partners that host (or are hosting) a third party payload. Restoration activities can include corrections for anomalies, calibrations, verification, and validation procedures.

There are three Subcategories within the Communications Category one of which applies to the SOC.

# Table 24 - Communications Subcategories

|  |  |  |
| --- | --- | --- |
| **Recover** : **Communications**  **Subcategory**  **Applicability to the SOC** | | **References** |
| **RC.CO-1: Public relations are managed.** | Not applicable to the SOC | **NIST SP 800-34 Rev. 2** 4  **NIST SP 800-53 Rev. 5** IR-4  **NIST SP 800-184** 2.4 |
| **RC.CO-2: Reputation is repaired after an incident.** | Not applicable to the SOC. | **NIST SP 800-53 Rev. 5** IR-4  **NIST SP 800-184** (all sections) |
| **RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.** | Communicate recovery activities to all relevant internal and external stakeholders, executive teams, and management teams. | **NIST SP 800-34 Rev. 2**  **NIST SP 800-53 Rev. 5** CP-2, IR-4  **NIST SP 800-184** |