Cislunar Incident Response Framework

Building for a Resilient Future in Cislunar Space

A Critical Study of Cislunar Response Applications in the International Space Economy

By
Nick Reese
Annslee Perego, Esq.

Research Assistant: Erik Rodriguez

Authors’ Note

The authors of this study would like to thank the Space ISAC and New York University’s Center for Global Affairs for their support to this project. We would also like to thank those who participated in any of the runnings of the Saving Selene tabletop exercise without which this study would not have been possible.

Abstract

Innovations and economic opportunities are making missions into cislunar space by commercial space operators a near term reality. Pushing into cislunar space will soon result in a sustained human presence in cislunar space requiring resilience and protection of the infrastructure that enables these missions. In 2024, the Space ISAC ran its *Saving Selene* tabletop exercise across three continents. This paper explores the findings of the exercises combined with incident response best practices from Earth. . There are no thoroughly developed incident response frameworks for cislunar space to guide response when an incident threatens an organization’s mission. This paper introduces a novel Cislunar Incident Response Framework (CIRF) that is inclusive of cislunar space’s unique characteristics and is adaptable for any organization venturing into cislunar space. The CIRF is intended to work as a list of well-thought-out recommendations that vary based on severity, incidents and phases. Specifically, this framework is formatted to flow through the prevention, identification, response and recovery for any incident in cislunar. The CIRF recognizes the dire importance of having an implemented incident response plan to be proactively prepared for inevitable incidents. By promoting information sharing and incident response standards, organizations endeavoring in cislunar are able to mitigate the losses such as human life, sensitive data, and machinery. As the first of its kind, this paper builds a framework by adapting incident response concepts tested on Earth and tailoring it for cislunar space.

About the Authors

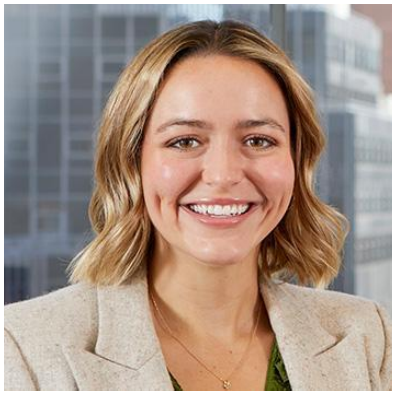
	
Nick Reese	**Annslee Perego, Esq.**
Nick Reese is the cofounder and COO of Frontier Foundry Corporation and a Strategic Advisor to the Space ISAC. He is a former federal government space policy maker and an adjunct professor at the NYU Center for Global Affairs.	Annslee Perego is a practicing attorney focusing on cybersecurity, privacy, and incident response. She is pursuing a Master of Science in Global Security, Conflict and Cybercrime at NYU, where she focuses her studies on national security and emerging technology. She is a graduate of Benjamin N. Cardozo School of Law.

Table of Contents Page

Introduction

For most of human history, space and its contents were the observable subjects of speculation and myth. In 1957, space became reachable, albeit for a small number of governments and a handful of supporting contractors. The late 2010s opened space to economic interests and commercial organizations marking a significant milestone in human history. The space economy is only a few years old, but it has already ushered in innovations that have dramatically dropped launch cost per kilogram leading to a dramatic increase in the number of satellites in low Earth orbit (LEO). LEO is now a commercial hub where economic value is being driven every day. Even with all of the activity, LEO is not the final destination. With planned missions to the Moon in 2026 on Artemis II, cislunar space is the next domain for space economic activity. Missions into cislunar space will require supporting infrastructure, and that infrastructure must be secure. We also need the ability to quickly and effectively respond to any incidents in cislunar space in an era where information is weaponized, cyberattacks are common, and geopolitical powers are competing in space.

Cislunar space brings with it a host of different challenges that are distinct from LEO. Missions to extract minerals or establish semi-permanent habitations on celestial bodies will return significant economic value, but it also comes with new risks. An incident in cislunar space may require space rescue, specialized communications relays, or other lifesaving measures in the event of a major outage. This paper examines the foundational readiness of space operators in the commercial sector to respond to complex incidents in cislunar space. This study was inspired by the Saving Selene tabletop exercise run by the Space ISAC in 2024 across three countries. The exercise identified numerous gaps across multiple organizations and skill sets that should be remedied before cislunar missions begin in earnest. The paper studies responses in that exercise alongside best in class incident response frameworks but adjusts for the needs of cislunar space. The result of the study is a cislunar incident response framework that can be used by the space community to build risk management frameworks and incident response guidance for cislunar flight.

The framework identifies general areas that assist in preparation, prevention, communication, and response to an incident. The study is broken into four sections:

- Prevention
- Identification
- Response
- Recovery

Each section provides specific guidelines that commercial space operators can use to improve their capacity to respond to cislunar incidents.

Given the complexities of commercial operations cutting across multiple nations, jurisdictions, investors, insurers, and militaries, the space economy must adopt a consistent approach to incident response in cislunar space. A consistent approach will create consistencies in incident reporting, information sharing, requests for assistance, and communication across multiple stakeholders. It will also help responders identify and mitigate against possible disinformation that could impede or hinder response operations.

The intent of this framework is to provide guidance upon which individual organizations can build tailored response guidance. Each commercial mission will have different stakeholders, goals, equipment, and nations involved making a monolithic approach unworkable. Instead, this research focuses on identifying those aspects that are critical to cislunar flight and incident response. This study comes with companion one-page documents with graphical representations of each section of this study. These documents are intended to be used as quick reference guides for operators working to respond to an incident. They are also intended as a visual representation of the findings of this study and to inspire the creation of organization specific incident response frameworks. Appendix 2 of this report provides a template for a cislunar incident report that may be used or adapted according to the needs of the specific organization.

Cislunar space will soon be an actuality and humanity will soon face the reality of having humans in cislunar space at a near constant rate. Incident response in cislunar space must be consistent and standard and must focus on those aspects of cislunar activity that are critical. The supporting infrastructure that will soon be in place must be secure, so it is available for incident response in the future. This study is the first step in creating a cohesive and consistent incident response plan for cislunar incidents. Further study is required on technical specifications that will enable response options such as space rescue and communications relays.

Scope

Develop a cislunar Incident Response Framework (CIRF) for incident response in cislunar space including practical tools to help organizations respond to attacks. This framework[1] is meant for use by all organizations, governmental, private and otherwise, who endeavor to launch missions in cislunar space. For the purposes of this document, "organization," is used to mean any private company, government or nongovernment agencies, or other organization conducting missions within cislunar space.

Definitions of Cislunar

[1] Jensen, Bob. "Critical Elements of Crisis Management." *Omnilert*, 2017. This incident response framework draws heavy inspiration from Jensen's incident response framework that has been implemented across the world.

The United States defines cislunar as “the region of space from the Earth out to and including the region around the surface of the Moon.”[2] Japan’s National Institute for Defense Studies defines cislunar as “the space on this side of the Moon (in Latin, ‘cis’ means ‘on this side of’). This includes the area of space from the Earth to geosynchronous orbit (GEO), but generally, the area within GEO is excluded when discussing cislunar space. On the other hand, definitions of cislunar space often include the five Earth-Moon Lagrange points (EMLs), their nearby orbits, and the Moon.”[3]

Purpose

A November 2022 White House press release stated, “NASA estimates that over the next ten years, human activity in cislunar space will be equal to or exceed all that has occurred in this region since the Space Age began in 1957.”[4] cislunar is ripe for exploration and technological advancement.[5]

Missions in cislunar space present specific challenges. cislunar has limited “real estate” available to place orbiting sensors due to few repeating natural orbits, and planned trajectories tend to drift due to instability.[6] Preparing for incidents that may result from these unique characteristics is vital to the future of space exploration. Traveling to cislunar space takes a minimum of three days,[7] which further emphasizes the importance of an incident response plan especially when humans are involved.

Prevention

The purpose of the preventative protocols are to provide considerations that should be adopted by organizations in preparation for an inevitable incident, including: **prediction, information sharing, policies, promotion & training, and partnerships.**

[2] 42 USC § 18302.

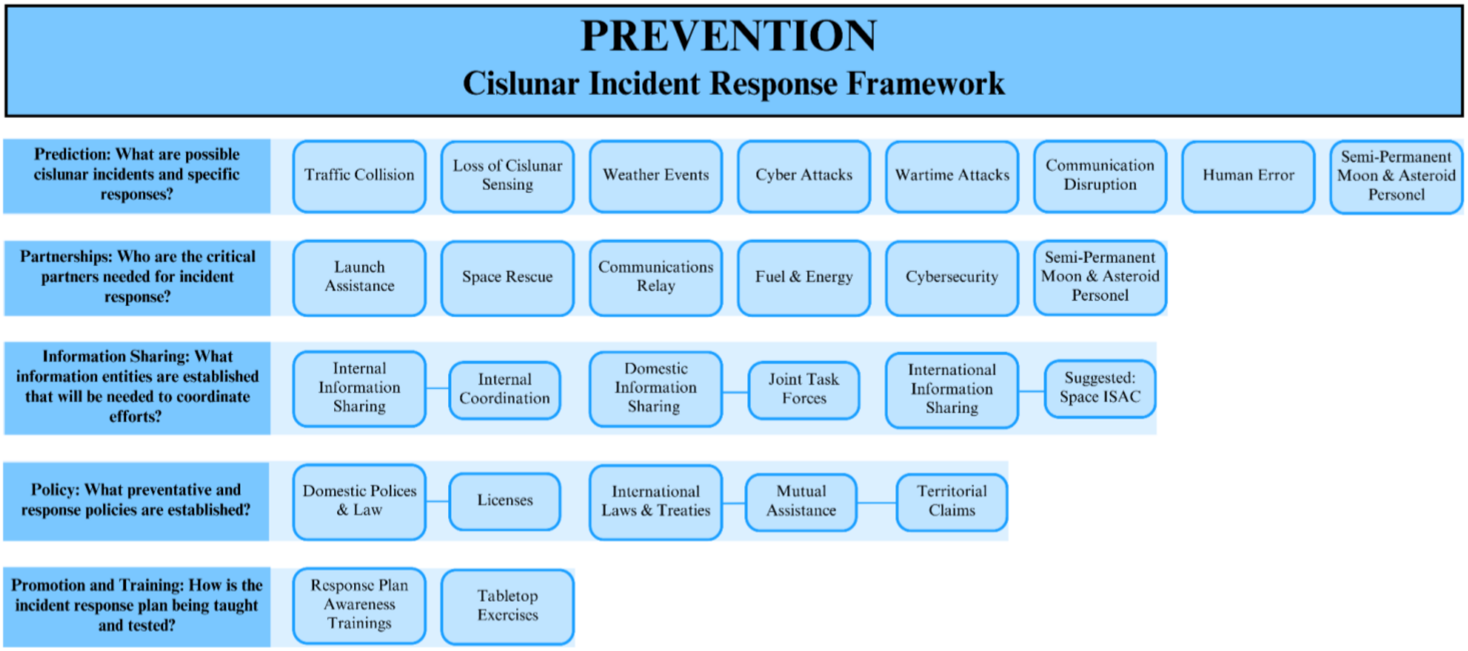
[3] Yasuhito, Fukushima, and Yatsuzuka Masaaki*. “Cislunar Security: U.S. and Chinese Activities in Cislunar Space and Future Issues.” p. 3. *National Institute for Defense Studies*, https://www.nids.mod.go.jp/english/publication/security/pdf/2024/04.pdf. Accessed 4 November 2024.

[4] “FACT SHEET: First National Cislunar Science & Technology Strategy.” *The White House*, The White House, 17 November 2022, https://www.whitehouse.gov/ostp/news-updates/2022/11/17/fact-sheet-first-national-cislunar-science-technology-strategy/.

[5] Cislunar Technology Strategy Interagency Working Group. “National Cislunar Science & Technology Strategy.” *The White House*, National Science and Technology Council, November 2022, https://www.whitehouse.gov/wp-content/uploads/2022/11/11-2022-NSTC-National-Cislunar-ST-Strategy.pdf. Accessed 29 November 2024. The United States recognizes cislunar as a space priority, and this document provides the United States’ first interagency strategy guide.

[6] Holzinger, M. J., et al. “A Primer on Cislunar Space.” p. 19. *Air Force Research Laboratory*, https://www.afrl.af.mil/Portals/90/Documents/RV/A%20Primer%20on%20cislunar%20Space_Dist%20A_PA2021-1271.pdf?ver=vs6e0sE4PuJ51QC-15DEfg%3D%3D. Accessed 3 11 2024.

[7] “It's International Moon Day! Let's talk about Cislunar Space.” *Medium*, 20 July 2023, https://medium.com/the-aerospace-corporation/its-international-moon-day-let-s-talk-about-cislunar-space-9d108f1a1b0b. Accessed 9 December 2024.



PREVENTION

Cislunar Incident Response Framework

Prediction: What are possible cislunar incidents and specific responses? — Traffic Collision; Loss of Cislunar Sensing; Weather Events; Cyber Attacks; Wartime Attacks; Communication Disruption; Human Error; Semi-Permanent Moon & Asteroid Personel

Partnerships: Who are the critical partners needed for incident response? — Launch Assistance; Space Rescue; Communications Relay; Fuel & Energy; Cybersecurity; Semi-Permanent Moon & Asteroid Personel

Information Sharing: What information entities are established that will be needed to coordinate efforts? — Internal Information Sharing – Internal Coordination; Domestic Information Sharing – Joint Task Forces; International Information Sharing – Suggested: Space ISAC

Policy: What preventative and response policies are established? — Domestic Polices & Law – Licenses; International Laws & Treaties – Mutual Assistance – Territorial Claims

Promotion and Training: How is the incident response plan being taught and tested? — Response Plan Awareness Trainings; Tabletop Exercises

Prediction

To inform the creation of an incident response plan, organizations should consider types of incidents that may arise and analyze how response to each incident may differ. This will help organizations to create a well-informed incident response plan that is proactive, rather than reactive. Types of incidents may include:

(1) Cislunar Traffic Collisions: Space debris, satellite collisions, and infrastructure conflicts due to uncoordinated traffic.[8]

(2) Cislunar Sensing: Inability to properly sense and monitor cislunar activity from Earth.[9]

(3) Weather-Related Events: Meteor showers, coronal mass ejections (CMEs).[10]

(4) Cyberattacks: Remote access hacking, distributed denial of service attacks, GPS spoofing, sensor manipulation, malware injection, etc.[11]

[8] Dr. Hedrick, Gabrielle. Phone Interview. 11 November 2024.

[9] Hedrick, Gabrielle. "Cislunar Space Situational Awareness." *MITRE | Solving Problems For A Safer World*, 2023, p. 3. 23-0595. Accessed 14 December 2024.

[10] "Coronal Mass Ejections | NOAA / NWS Space Weather Prediction Center." *Space Weather Prediction Center*, https://www.swpc.noaa.gov/phenomena/coronal-mass-ejections. Accessed 17 November 2024.

[11] *See*, Biden, Joe. "Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity." Th*e White House*, 16 January 2025, https://www.whitehouse.gov/briefing-room/presidential-actions/2025/01/16/executive-order-on-strengthening-and-promoting-innovation-in-the-nations-cybersecurity/. Accessed 18 January 2025.This executive order emphasizes the importance of space cybersecurity and orders

(5) Human Errors: Improper training, insider threats, and operational mistakes.

(6) Wartime: Deliberate interference with spacecraft or lunar infrastructure.

(7) Communications Disruption: Disinformation attacks, loss of communications.

Organizations should maintain a descriptive list of possible incidents including potential vulnerabilities and resources needed to respond. Organizations may consider creating standard operating procedures (SOP) for incidents with higher likelihoods.[12] A SOP should include trigger points for activation and key steps to respond to the situation.

Information Sharing

(1) Internal Information Sharing Coordination: Organizations should have clearly defined roles and policies

for information sharing related to incidents. Having an information sharing plan is crucial, as cislunar space has the potential to house critical infrastructure and research opportunities. Organizations should establish internal procedures for sharing with domestic and international information sharing organizations and other partnerships.

(2) Domestic Information Sharing Organization: States should consider creating joint task forces (JTF) to better coordinate resources and communications similar to the United States' National Cyber Investigative Joint Task Force.[13] In response to cyber-attacks, the United States has assembled a National Cyber Investigative Joint Task Force (NCIJTF). With "over 30 partnering agencies from across law enforcement, the intelligence community, and the Department of Defense, the primary responsibility of the NCIJTF is "to coordinate, integrate, and share information to support cyber threat investigations, supply and support intelligence analysis for community decision-makers, and provide value to other ongoing efforts in the fight against the cyber threat to the nation." As space exploration increases in frequency, states should consider implementing a similar space JTF with the goals of establishing clear lines of communication, exposing weaknesses, improving response time, and developing collaborative relationships.

(3) International Information Sharing Organization: This organization should be created to house information sharing[14] that does not depend on alliances nor treaties between friendly nations but

government agencies to make recommendations to the Federal Acquisition Regulatory (FAR) Council to update civil space contract requirements to include cybersecurity measures.

[12] "Tips for Creating Standard Operating Procedures." *American Bar Association*, https://www.americanbar.org/groups/government_public/resources/practice_pointers/tips-creating-SOPs/. Accessed 7 December 2024.

[13] *See,* "National Cyber Investigative Joint Task Force — FBI." *FBI*, https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force. Accessed 10 December 2024.

[14] Cislunar Technology Strategy Interagency Working Group. "National cislunar Science & Technology Strategy." p. 13. *The White House*, National Science and Technology Council, November 2022, https://www.whitehouse.gov/wp-content/uploads/2022/11/11-2022-NSTC-National-cislunar-ST-Strategy.pdf.

rather for the betterment of cislunar space. This organization should concentrate on three priorities: (1) tracking the status of cislunar missions, (2) information gathering about common IT issues and cyberattacks, and (3) issuing safety certificates for missions.

(a) Tracking the status of cislunar missions would help alert other organizations of potential incidents. This provides world partners notice of cislunar missions, which allows international incident response assistance to be on alert

(b) Information sharing about common IT issues and potential cyberattacks helps the international community to better prepare infrastructure to be resilient to these types of issues and prevent a larger incident. This would operate similarly to the Cybersecurity & Infrastructure Security Agency's "Known Exploited Vulnerabilities Catalog,"[15] which publishes cyber threats to put critical infrastructure on alert of possible vulnerabilities.

(c) Issuing safety certificates, while not meant to be an enforcement mechanism, could serve as an accountability mechanism that missions established preventative measures and an incident response plan.

The Space ISAC would be an ideal home for this organization. While the Space ISAC is a membership organization, it is an ideal organization because it is not nationally aligned unlike a government organization. The Space ISAC is more ideal than creating a body within the United Nations, because it is not politicized, and it is academically focused. The Space ISAC is well-positioned to expand around the world creating an international, neutral information sharing hub.

Members of the Space ISAC could adopt policies similar to the Artemis Accords. For example, the Artemis Accord signatories "commit to taking all reasonable efforts to render necessary assistance to personnel in outer space who are in distress and acknowledge their obligations under the [agreement]."[16] Having a neutral body would allow members to build mutual assistance policies for personnel and critical infrastructure and collaborate on cislunar exploration.

Policies

(1) Domestic Policies and Law:[17] In the United States, the Federal Aviation Administration (FAA) requires a license covering pre- and post-flight operations. To obtain the license, applications must provide proof of some incident response planning for human space flight.[18] Additionally,

Accessed 29 November 2024. The United States has already emphasized the importance of coordinating cislunar activities.

[15] "Known Exploited Vulnerabilities Catalog." *CISA*, https://www.cisa.gov/known-exploited-vulnerabilities-catalog. Accessed 9 December 2024.

[16] NASA. *The Artemis Accords*. p. 3. 2020. *NASA*, NASA, https://www.nasa.gov/wp-content/uploads/2022/11/Artemis-Accords-signed-13Oct2020.pdf?emrc=673a66924cd64. Accessed 17 November 2024.

[17] This category encompasses policies that could form the basic requirements for issuing safety certificates.

[18] *See* 14 CFR 460.5.

applicants must provide proof of financial responsibility and allocation of risk[19] and meet safety requirements to obtain a license.[20] The below suggestions are based in part on the FAA regulations; however, they should be applied to all cislunar endeavors, manned or unmanned, and adopted internationally.

(a) Proof of Incident Response Plan: every organization endeavoring to launch a mission into cislunar space should have an incident response plan in place. Suggestions for an incident response plan are more fully explored later in this document.

(b) Proof of Funding: organizations should secure funding for the entirety of the mission, which includes funding for backups should an incident occur. Proof of funding should include agreements with other organizations that have agreed to assist in case of emergency.

(c) Critical Infrastructure Redundancy Plan: organizations should identify critical infrastructure and include redundancies in the case of failure. A redundancy is "the ability to utilize backup systems for critical parts of the system that fail."[21] The Department of Transportation's system redundancy and resilience plan includes developing redundancies in several areas including having additional trained staff and redundant equipment and supplies.[22]

(2) International Law:[23] Organizations should evaluate international law to understand the current parameters of mutual assistance and territorial claims to inform incident response planning.

Promotion and Training

Promotion of incident response frameworks ensures that all stakeholders, both private and public, are prepared for a crisis in cislunar. Marketing campaigns help educate public and private partners about expectations for cislunar space exploration. Education also helps to prevent disinformation and foster public trust.

To test the efficacy of developed incident response frameworks, educational training should be implemented. Organizations should engage in Scenario-Based Tabletop Exercises & Awareness Trainings to test the strength of an incident response plan.

[19] *See* 14 CFR 440.

[20] *See* 14 CFR 450.101-189.

[21] U.S. Department of Transportation. "6.8 System Redundancy and Resiliency." *U.S. Department of Transportation Federal Highway Administration*, U.S. Department of Transportation, 7 February 2006, https://ops.fhwa.dot.gov/publications/fhwahop08015/lit6_8.htm.

[22] U.S. Department of Transportation. "6.8 System Redundancy and Resiliency." *U.S. Department of Transportation Federal Highway Administration*, U.S. Department of Transportation, 7 February 2006, https://ops.fhwa.dot.gov/publications/fhwahop08015/lit6_8.htm.

[23] *See* Appendix 1 for further reading on current international treaties and legal parameters affecting incident response.

(1) Awareness Training: Educate individuals and partners involved with the mission about the incident response plan, including appropriate channels of communication. Training may include:

(a) Procedures Awareness: Train incident response personnel on the procedures in place for incident response including communication, identification, and response procedures

(b) Disinformation Awareness:[24] Expose incident response personnel to disinformation campaigns, strategies, and tactics to improve their judgment and ability to discern factual information and disinformation.

(2) Tabletop Exercises: Conduct regular drills to simulate potential cislunar incidents, training personnel and organizations for real-world scenarios.

(a) Example Scenario: A cyberattack targets cislunar satellites, specifically their sensors, with the hopes of causing them to input inaccurate information to cause a collision or disrupt scientific research. Your task is to identify the source of the attack, coordinate with international stakeholders to mitigate the impact, restore functionality, and assess areas for improvement.

Partnerships

Organizations should maintain contacts for partnerships in case of an incident.[25] Partnerships should include organizations that have agreed to aid in mutual assistance should an incident arise. Every organization should consider these categories of partners:

(1) Launch Assistance: Aid in the launch and return phases.

(2) Space Rescue: Delivers aid in the case of an incident post launch.

(3) Communications Relay: Ensures the integrity and resiliency of communication channels.

(4) Cislunar space Repair: Involves in emergency repairs to critical infrastructure of manned and unmanned spacecraft.

(5) Fuel and Energy: Facilitates the proper amount of power sources for all aspects of the spacecraft in cislunar, including plans for emergency fueling.

(6) Cybersecurity:[26] Maintains the integrity of critical systems in cislunar and responds to incidents in real time.

[24] *See* Roozenbeek, Jon, et al. “Prebunking interventions based on “inoculation” theory can reduce susceptibility to misinformation across cultures.” *Misinformation Review*, Harvard Kennedy School, 3 February 2020, https://misinforeview.hks.harvard.edu/article/global-vaccination-badnews/. Accessed 14 December 2024.

[25] *See* Appendix 1(a). The Outer Space Treaty and Artemis Accords include mutual assistance clauses for incidents involving astronauts. For the purposes of this framework, mutual assistance should be considered for astronauts and unmanned spacecrafts, particularly spacecrafts affecting critical infrastructure.

[26] Organizations should prioritize the cybersecurity of itself and partners. Highlighting the import of cybersecurity, United States President Joe Biden issued an Executive Order on January 16, 2025, requiring cybersecurity measures

(7) Semi-Permanent Moon and Asteroid Personnel: Serves as support for all the functions listed above while also being a part of redundancy measures for incident response protocols.

(8) Information Sharing: Shares information with relevant stakeholders including public and private organizations that may assist with incident response.

Organizations may consider partnerships from a variety of industries to fulfill needs as outlined above. These partnerships may include:

(1) Private Industry Partners: Create defined partnerships with private companies.

(2) Domestic Government Partnerships: Identify the home state's government organizations including agencies, military resources, and other departments that can provide resources and assistance.

(3) International Government Partnerships: Identify other states that may be obligated by mutual assistance agreements or form partnerships with other states for these purposes.

(4) Academic Partnerships: Identify academic partnerships with universities, think tanks, and other bodies like the Space ISAC that can provide research about possible incidents to inform incident response plans and information necessary to inform active decision making during an incident.

Organizations should have a prioritized list of partnerships. Should an incident arise, the organization should have appropriate partners identified as first points of contact before escalating to additional partnerships. For example, an organization may be closely partnered with a private company and elect to contact that partner first. If the need is greater than the private company can meet, then the organization should have defined the next line of contacts such as domestic government and international government contacts.

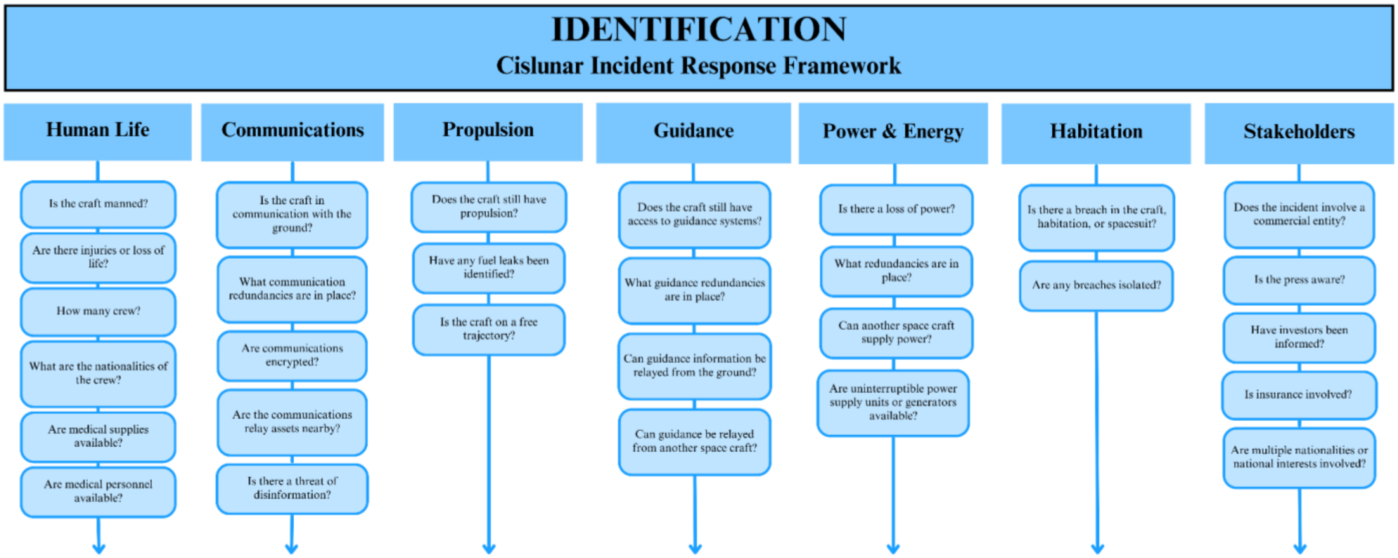
Identification

The first moments of an incident in cislunar space are crucial to how the incident is handled and what resources are brought to bear making the quick and accurate identification of the problem a primary concern for incident responders. The issue should be immediately assessed to understand the scope and cause. This section provides a logical flow that incident responders can use in the first moments of an incident to provide accurate and timely reports of the incident and request the correct support to solve the problems at hand. Incident responders should consider the potential impact of disinformation on a cislunar incident. This section also provides explicit guidance for verifying information received during an incident to guard against making decisions based on disinformation.

The CIRF is designed to provide guidance on those elements of a spacecraft that are most critical to its continued function and ability to sustain human life in the earliest moments of an incident. This will drive consistent reporting across the commercial, civil, and government sectors for smoother

such as backups, encryption, communication verification, and secure software and hardware are implemented as a requirement for civil space contracts through the FAR Council, *supra* note 11.

communication and information sharing. As more organizations adopt this approach, the identification of the problem will become quicker and more accurate. It will also help responders properly diagnose issues and differentiate between cybersecurity events versus systems failures or other issues with the spacecraft. In an era where the commercial footprint in space is expanding while geopolitical competition in space is rising, it is critical that commercial space operators have systems in place to properly identify incidents and quickly share consistent information with the correct stakeholders. This will build value in the space economy by introducing more security and resilience while shortening the time to respond to an incident.


IDENTIFICATION

Cislunar Incident Response Framework

Human Life

- Is the craft manned?
- Are there injuries or loss of life?
- How many crew?
- What are the nationalities of the crew?
- Are medical supplies available?
- Are medical personnel available?

Communications

- Is the craft in communication with the ground?
- What communication redundancies are in place?
- Are communications encrypted?
- Are the communications relay assets nearby?
- Is there a threat of disinformation?

Propulsion

- Does the craft still have propulsion?
- Have any fuel leaks been identified?
- Is the craft on a free trajectory?

Guidance

- Does the craft still have access to guidance systems?
- What guidance redundancies are in place?
- Can guidance information be relayed from the ground?
- Can guidance be relayed from another space craft?

Power & Energy

- Is there a loss of power?
- What redundancies are in place?
- Can another space craft supply power?
- Are uninterruptible power supply units or generators available?

Habitation

- Is there a breach in the craft, habitation, or spacesuit?
- Are any breaches isolated?

Stakeholders

- Does the incident involve a commercial entity?
- Is the press aware?
- Have investors been informed?
- Is insurance involved?
- Are multiple nationalities or national interests involved?

Human Life

The presence of human lives onboard the spacecraft and the condition of those humans should always be the first consideration and will drive the urgency and support functions required to respond to the incident. Incident responders should immediately seek to determine the presence and condition of human life aboard the spacecraft as well as the ability to administer lifesaving aid in flight. For organizations creating their own incident response frameworks and reporting mechanisms, human life should be the first consideration and conditions should be immediately reported through information sharing, government, and public communications channels.

Communications

Communications with the ground, other spacecraft, between astronauts, and with habitations is a critical capability, the disruption of which would result in limitations on incident responders and potentially cascading failures. The state of the communications with the spacecraft should be evaluated immediately upon learning of a cislunar incident. Responders should seek to identify potential communications relays or other assets that can assist in restoring or building further redundancy in communications. The status of the craft's communications should also be reported as a primary evaluation criterion in the first reports of the incident regardless of reporting channel.

Propulsion

Propulsion systems have been recognized as critical since the beginning of space flight and often have redundancies built in. An outage in a propulsion system could critically endanger the mission and its crew if not diagnosed quickly. The state of the propulsion system should be included as a part of the initial assessment of the incident and communicated consistently to all stakeholders. The propulsion issue may also give an indication on whether a space rescue is necessary or feasible. An issue with propulsion should also necessitate a review of applicable treaties and laws to determine how a rescue may be affected and what parties are available to assist.

Guidance

Similar to propulsion, a significant failure in a guidance system may necessitate extreme measures to save the craft. Guidance should likewise be immediately evaluated in the early moments of the incident to give planners a full picture of the threat to the craft and its crew.

Power and Energy

Power and energy to habitations is an essential component of their resilience. A loss of energy and power affects communications, propulsion, and all other energy dependent operations. It is necessary to identify any power & energy failures or vulnerabilities and facilitate the other means of supply such as the use of uninterruptible power supply units and generators.

Habitation

Habitation refers to the structural integrity of a craft in orbit or in transit, a stationary structure on a cislunar body, and spacesuits for humans. The structural integrity of any habitation in the cislunar environment is critical to the continued function of critical systems and to human life. Any damage to the physical structure of any habitation should be immediately evaluated and reported as a critical issue in the first reports of the incident.

Stakeholder Identification

With more participants in the space economy comes more complexity in stakeholder identification. Stakeholders should be considered from concerned companies, government agencies, nations, investors, insurance companies, academia, and more. A consistent checklist enabling rapid and accurate stakeholder identification will improve information sharing and, by extension, the quality and speed of responses to potentially life-threatening incidents.

Disinformation

If the incident involves information technology or telecommunications, the information should first be verified through separate channels to prevent disinformation and inform accurate decision making. Combatting disinformation could be the critical piece that determines the success of an incident response. "The increasing complexity of our low-Earth-orbit (LEO) environment, combined with the militarization of the space domain by major powers, all but assures that disinformation in the space domain will be a factor in space incident response," and "the proliferation of disinformation campaigns creates an environment where the responses to incidents in space could be slowed just enough for critical lifesaving decisions to be delayed—or for decisions to be made on misleading information with potentially catastrophic results."[27] In order to verify information, the following steps should be followed:

(1) Identify inconsistencies: Look for discrepancies in data, sudden changes in patterns or information that contradicts established facts.

   (a) Keep records of inconsistencies that may present over time. Records of small inconsistencies may be used to determine whether an issue is the result of a system malfunction or coordinated cyber-attack.

(2) Verify sources: Verify incoming information via a secondary channel.

   (a) Multiple communication channels should be established on separate networks. The multiple channels can be utilized to verify information without fear of poisoning from one potentially infected channel. Incorporating redundancies into communication channels is essential to communications resilience.

(3) Analyze impact: Evaluate the potential consequences of the manipulated information on decision-making processes and outcomes.

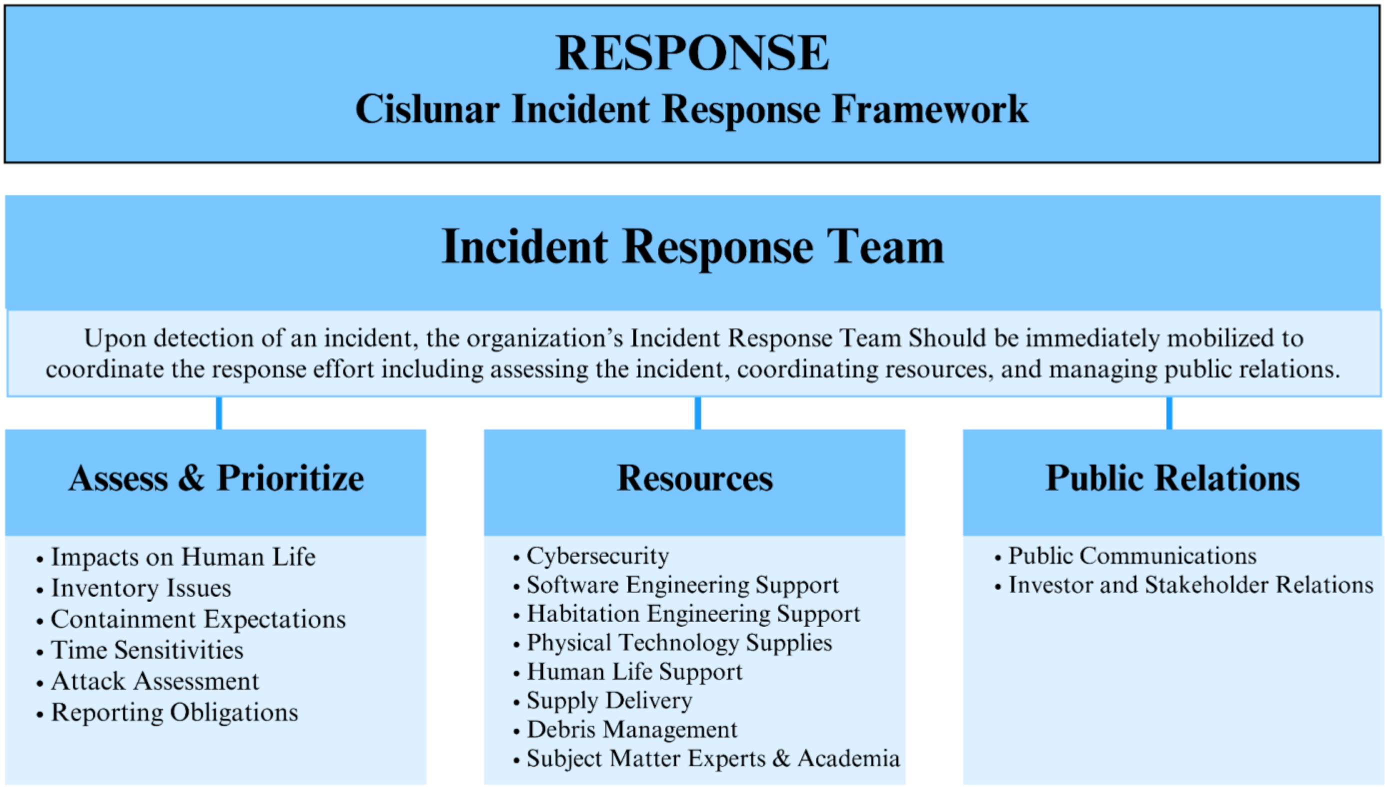
(4) Investigate motive: Consider who benefits from the manipulated information and their possible motivations.

[27] Reese, Nick, and Christina Nemr. "Stellar Deception: Disinformation's Threat to Effective Space Incident Response." *The Cyber Edge by Signal*, 1 November 2024, https://www.afcea.org/signal-media/cyber-edge/stellar-deception-disinformations-threat-effective-Space-incident-response. Accessed 4 November 2024.

(5) Map the physical location of inconsistencies to identify the main target if this is the result of a cyber-attack.[28]

Response

Following the initial identification phase of the incident, organizations will move into the response portion of addressing the incident. Whether involving manned or unmanned habitations, a clear plan of response will aid in tactfully resolving an incident. The following elements are meant to guide organizations development of a response framework by highlighting critical aspects. This response framework is not meant to be all inclusive, but the framework is malleable to organizations' unique and specific needs.



RESPONSE

Cislunar Incident Response Framework

Incident Response Team

Upon detection of an incident, the organization's Incident Response Team Should be immediately mobilized to coordinate the response effort including assessing the incident, coordinating resources, and managing public relations.

Assess & Prioritize

- Impacts on Human Life
- Inventory Issues
- Containment Expectations
- Time Sensitivities
- Attack Assessment
- Reporting Obligations

Resources

- Cybersecurity
- Software Engineering Support
- Habitation Engineering Support
- Physical Technology Supplies
- Human Life Support
- Supply Delivery
- Debris Management
- Subject Matter Experts & Academia

Public Relations

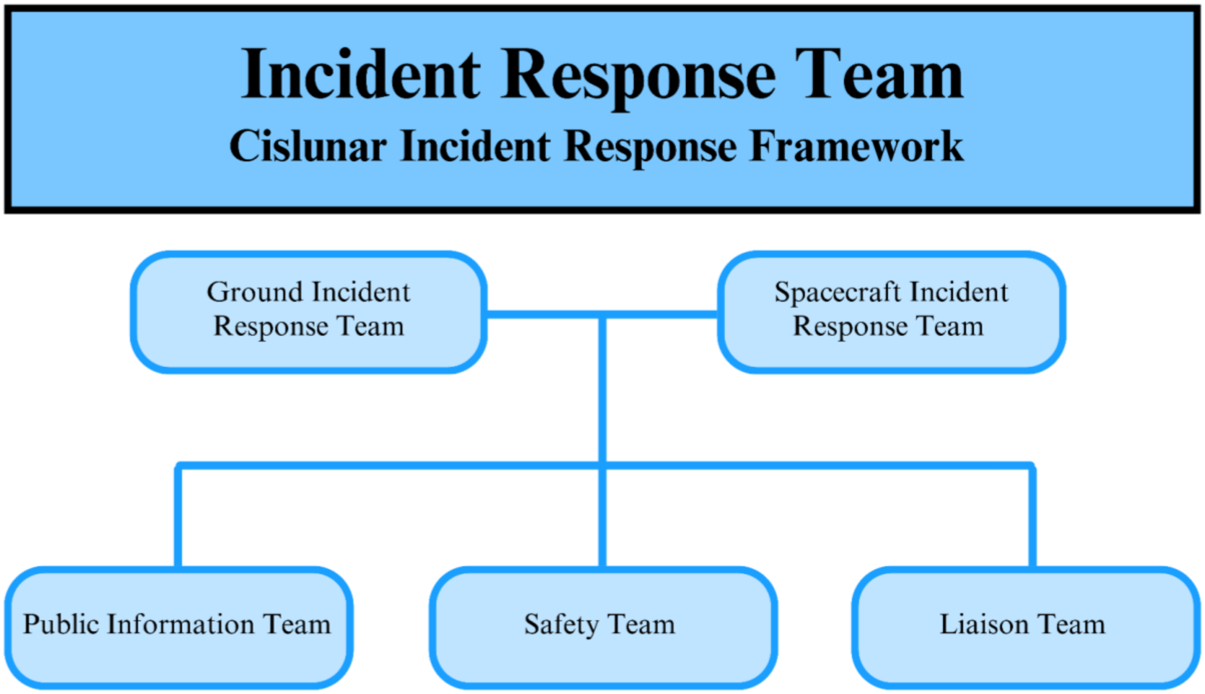
- Public Communications
- Investor and Stakeholder Relations

Incident Response Team

Whether or not an incident involves a communications issue, an established incident response team should be quickly mobilized. An incident response team should be tailored to the organization, and this suggested organization is meant to be adaptable based upon the organization's structure. The below

[28] *See* Reese and Nemr for the original disinformation framework that was adapted for this document, *supra* note 27

guidance is an incident response team structure similar to the Federal Emergency Management Agency's Incident Command System, which has been duplicated across industries because of its effectiveness.[29]


Incident Response Team
Cislunar Incident Response Framework
Ground Incident Response Team
Spacecraft Incident Response Team
Public Information Team
Safety Team
Liaison Team

(a) Ground and Spacecraft Incident Response Team: The Ground Team coordinates issues on earth, while the Spacecraft Team consists of individuals currently in cislunar space, if applicable. Both teams work together to coordinate ground and space effort, respectively.[30] These teams are responsible for approving the incident response plan and overseeing the coordination of the plan. These positions are also responsible for gaining approval and coordinating with the organization's regular chain of command.

(b) Public Information Team: This team is responsible for obtaining accurate information for press releases and coordinating with news organizations. The role also encompasses maintaining accurate information about the incident and reporting data to the International cislunar Information Sharing Organization, suggested to be the Space ISAC, for purposes of tracking vulnerabilities over time.

(c) Liaison Team: This position is responsible for coordinating with industry partners, government organizations, and academic bodies as resources are needed at the directions of the Ground and Spacecraft Incident Response Teams.

[29] Federal Emergency Management Agency. "ICS Organizational Structure and Elements." *FEMA*, March 2018, https://training.fema.gov/emiweb/is/icsresource/assets/ics%20organizational%20structure%20and%20elements.pdf. Accessed 10 December 2024.

[30] If there is no manned spacecraft involved, then the Ground Incident Response Team subsumes the entirety of the role.

(d) Safety Team: This position is responsible for identifying hazards and the resources needed to respond. This position should take an active role in reviewing any incident response plan for safety considerations.

Assess and Prioritize

The incident response team should first work to assess the scope and cause of the issue to develop a response plan. An incident in cislunar may require a complex response plan; hence, assessing the initial scope and cause of the incident will help organizations to formulate a more robust and proactive plan.

(a) Human Life: Are personnel involved? How may this incident impact their safety?

(b) Inventory Issues: What are the verified issues? What are the unknowns?

(c) Containment: What steps can be immediately taken to prevent further harm? For example, can devices infected with malware be turned off to prevent the spread? Can an affected portion of the habitation be closed off?

(d) Time Sensitivity: How much time is available before the incident seriously threatens habitation or human life? If resources need to be transported to the habitation, how long will this take?

(e) Attack: Is this an attack from a bad actor? Or can this be attributed to an unanticipated issue, human error, or system failure?

(f) Reporting: Gather the information available and provide an initial incident response in a standardized format to identified stakeholders in a timely manner.

Resources

Organizations will need to quickly identify the resources needed to respond to the incident. This includes an assessment of what resources are available, what are the limits of available resources, and what resources are needed. For resources needed, organizations will need to identify sourcing from internal supplies or partnerships as discussed in the prevention section of the CIFR. Specific categories of resources may include:

(a) Cybersecurity: Incidents may involve malicious actors that deploy malware, or it may be the result of a technology failure. Cybersecurity personnel, such as software engineers and threat intelligence analysis, can help determine cyber risks and secure systems. Cybersecurity personnel will also be critical if communication channels are impacted, and there is a need to verify whether communications from the habitation to earth are accurate.

(b) Software Engineering Support: If the information technology (IT) or operational technology (OT) for a habitation is impacted, it will be necessary to have software engineering support to help secure and restore these systems. This could involve issues with navigation and trajectory systems, sensors, and other critical technologies.

(c) Habitation Engineering Support: If the physical technology (PT) of the habitation fails, support from electrical, mechanical, aerospace, and other engineers may be necessary to repair PT issues. PT issues may involve propulsion or other structural integrity issues.

(d) Physical Technology (PT) Supplies: This involves tangible supplies that may be needed to repair habitation structures or restore function. This may involve issues with structural integrity of a habitation, propulsion mechanical parts, etc.

(e) Human Life Support: Resources including medical doctors, medical supplies, food, water, oxygen, spacesuits, and other human life supporting means may need to be sourced to respond to issues involving human life.

(f) Supply Delivery: Physical ability to deliver the resources necessary to respond to the incident within any time sensitivity constraints.

(g) Debris Management: Coordinate resources necessary for debris removal that may have resulted to mitigate future debris-related incidents and keep the cislunar environment healthy.

(h) Subject Matter Experts and Academia: These resources are essential to providing response solutions to novel incidents. These experts may also be consulted in the event research & development projects are at risk.

Public Relations

Organizations need to consider the impact of communicating details of the incident to various communities, especially if the incident is the result of an attack. Attacks involving human life or critical infrastructure may be particularly sensitive if considered an act of war.[31] Incidents not considered to be the result of an attack may still involve sensitive information related to critical infrastructure, national security, or research and development. Intentional communications are a necessary and critical part of response to protect sensitive information, combat disinformation, and aid in response.

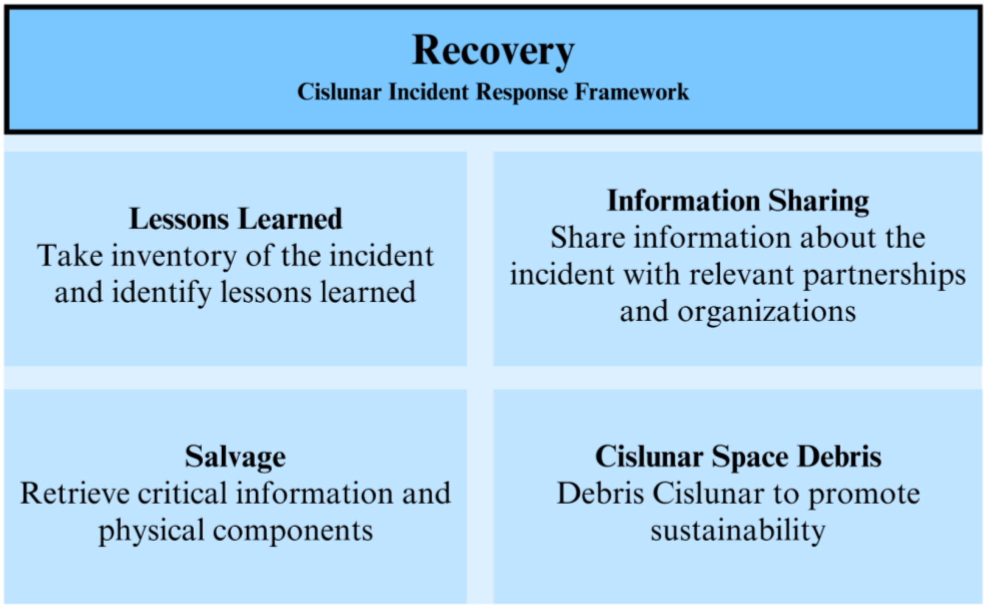
[31] *See* 18 U.S. Code § 2331. The United States defines an act of war as “any act occurring in the course of— (A) declared war; (B) armed conflict, whether or not war has been declared, between two or more nations; or (C) armed conflict between military forces of any origin.”

(a) Public Communication: Messaging for news outlets to accurately and strategically report incidents. Organizations should consider the sensitivity of attributing the incident as an attack and determine what information is appropriate for public release as to not impact the response.

(b) Investor and Stakeholders Relations: Organizations may choose that the messaging for investors and stakeholders is more forthcoming about the details of the incident than public communications. Investor and stakeholder relations may impact the availability of funding or resources needed to respond to the incident.

Recovery

The recovery portion of CIRF aims to help prevent an incidents' recurrence through reflecting upon areas of improvement and gaps in an organizations' preparedness. These steps are meant to be taken after the incident is fully mitigated to allow the organization full understanding of how to prevent future incidents.



Recovery
Cislunar Incident Response Framework

Lessons Learned
Take inventory of the incident and identify lessons learned

Information Sharing
Share information about the incident with relevant partnerships and organizations

Salvage
Retrieve critical information and physical components

Cislunar Space Debris
Debris Cislunar to promote sustainability

Lessons Learned

Organizations should take inventory of the incident to identify lessons learned and improve response by conducting comprehensive assessments and debriefs with associated parties involved in the incident. Organizations may focus on the following key areas to understand the root cause of the incident and develop preventative future plans[32]:

(a) Material: Every PT, OT, and IT component involved that may have contributed to the incident.

(b) Procedures: The existing procedures governing the flow of information, incident response, operational protocols, etc. that may be improved to prevent a future incident.

(c) Nature: Any weather events in cislunar that may have contributed to the incident or other characteristic of the cislunar environment that was not previously adequately accounted for.

(d) Human Error: The human failures that may have contributed to the incident.

(e) Partnerships: Identify areas for improvement, including whether there are any gaps in the organization's preparedness that may require additional partnerships or a revision to procedures, such as best practices for communications to maximize efficiency during an incident.

Once these components are analyzed, the organization may update policies and procedures, evaluate the sufficiency of partnerships, conduct table-top exercises, improve technology, or train/retrain staff based on the lessons learned.

Information Sharing

Organizations may choose to share information to aid the greater cislunar community to prevent similar incidents. As previously suggested, the Space ISAC is a strategic organization that could catalogue incidents to improve resiliency in cislunar and identify trends of any recurring incidents, especially incidents involving cybersecurity. Organizations may also inform government organizations and industry partners of incidents and known vulnerabilities.

Salvage

This process plays a significant role in retrieving critical components, including physical technology and data. Similar to collecting the black box from a crashed airplane,[33] salvaging can provide pertinent information about the incident's causation, such as human error and system malfunctions, which will help inform lessons learned briefings.

[32] Key areas are largely influenced by the Ishikawa Diagram method which contains key elements to evaluate the cause of an incident. *See* 50MINUTES. *Ishikawa Diagram: Anticipate and Solve Problems Within Your Business*, p. 5. Lemaitre Publishing, 2015. *ProQuest Ebook Central*, https://ebookcentral.proquest.com/lib/nyulibrary-ebooks/detail.action?docID=4005660.

[33] "Black box flight recorder invented." *National Museum of Australia*, https://www.nma.gov.au/defining-moments/resources/black-box-invented. Accessed 28 January 2025.

Cislunar Space Debris

A component of salvaging may also include removing debris from cislunar space, which may prevent future incidents and promote good-will environmental practices. Low Earth Orbit is already considered "an orbital space junk yard,"[34] and preventing similar occurrences in cislunar is important as debris can cause catastrophic collisions. Organizations should endeavor to keep cislunar sustainable[35] for the health and viability of future missions.

Conclusion

In 2024, the Space ISAC created the *Saving Selene* tabletop exercise (TTX) to measure the ability of commercial space operators to identify, respond to, and coordinate during an incident in cislunar space. The TTX was run on three continents with a vast and diverse array of participants and observers. This study, commissioned by the Space ISAC, was intended to synthesize and analyze the body of information on incident response on earth, the realities of cislunar space, and what was learned through the TTXs to provide actionable steps to the commercial space economy. The goal of the TTX and of this study is to help space operators build processes and training programs to quickly and effectively respond to an incident in cislunar space that will save lives, equipment, and economic value in the very near future. The findings of this study illuminate some key factors for the community to consider:

(1) Standardization of Reporting: The space economy should work to standardize its reporting and communications for cislunar incidents before there is a sustained human presence in cislunar space.

(2) Incident Identification: Incident response must address the core problem and not the symptoms. Understanding when a craft is under cyberattack versus having a systems issue is key to effective incident response.

(3) Disinformation: Information is being weaponized and the space domain is one of geopolitical competition. The space economy must work to refine processes for the identification and mitigation of disinformation in an incident response situation.

(4) Cybersecurity: The space economy must invest in cybersecurity technology and workforce to build resilience against cyberattacks against cislunar systems.

(5) Prevention: Frameworks and processes that take a proactive approach to cislunar incident response are key to minimizing damage and saving lives.

The space community has always been defined by its resilience and redundant systems. That continues today in the engineering of craft and innovations that have enabled the growth in the space economy. That same mentality must be present in how the individuals on the ground approach an incident beyond LEO. Humanity is not far removed from a future where there will be a consistent presence of

[34] "Space Debris." *NASA*, 3 November 2023, https://www.nasa.gov/headquarters/library/find/bibliographies/Space-debris/. Accessed 31 January 2025.

[35] Margetta, Robert. "NASA-Supported Studies Will Focus on Addressing Space Debris." *NASA*, 28 July 2023, https://www.nasa.gov/organizations/otps/nasa-supported-studies-will-focus-on-addressing-Space-debris/.

humans in cislunar space. This future carries significant opportunity for economic growth, but only if resilience is built into the economic system as a primary feature. This study recommends the implementation of the CIRF as a starting point for organizations to tailor specific incident response teams, processes, and communications strategies. The CIRF recognizes that different cislunar missions will have different requirements and does not attempt to prescribe a one size fits all solution.

The CIRF's effectiveness is strengthened if entities collaborate to proactively prepare for cislunar incidents. The CIRF is intended to work as a list of well-thought-out recommendations that vary based on severity, incidents, and phases. By promoting information sharing and incident response standards, continuous exploration and investment into cislunar will be more resilient to incidents. This framework is meant to be dynamic, allowing for change and improvements that evolve with keeping up with the pace of technological advancements and increase presence in cislunar space. The CIRFs lifecycle is malleable, allowing for updates, additions and considerations, to tackle the constantly changing landscape of risks and vulnerabilities in cislunar space. The authors look forward to building upon the CIRF in partnership with government, private sector, and academic partners to sustain economic value in the space domain for decades to come.

APPENDIX 1

International Law

International Law was considered during the development of this framework. Specifically, mutual assistance and territorial claims are ripe for discussion as cislunar expeditions increase.

Mutual Assistance

In 1959, the United Nations General Assembly created the Committee on the Peaceful Use of Outer Space (COPUOS) to govern exploration and use of Space, which has to date, passed five treaties.[36] Of note, is The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, "The Outer Space Treaty of 1967."

Article V of The Outer Space Treaty declares, "States Parties to the Treaty shall regard astronauts as envoys of mankind in outer Space and shall render to them all possible assistance in the event of accident, distress, or emergency landing on the territory of another State Party or on the high seas."[37] The treaty incorporates the principle of mutual assistance[38][39] in regard to astronauts, but this treaty was signed in 1966 and did not contemplate the interconnected nature of critical infrastructure[40] on earth and in Space. As exploration continues, critical infrastructure on earth will become increasingly dependent on Space infrastructure. Consider how Global Positioning Systems[41] and the Internet[42] may become dependent on infrastructure within Space. An incident involving critical infrastructure could be devastating, and in response, the UN should explicitly include rendering all possible assistance in the event of an incident involving critical infrastructure.

[36] "COPUOS." *United Nations Office for Outer Space Affairs*, United Nations, https://www.unoosa.org/oosa/en/ourwork/copuos/index.html. Accessed 17 November 2024.

[37] United Nations. "Outer Space Treaty." *UNOOSA*, 19 December 1966, https://www.unoosa.org/oosa/en/ourwork/Spacelaw/treaties/outerSpacetreaty.html. Accessed 20 November 2024.

[38] NASA. "The Artemis Accords." *NASA*, 2020, https://www.nasa.gov/wp-content/uploads/2022/11/Artemis-Accords-signed-13Oct2020.pdf?emrc=675a3f85bf66a. The Artemis Accords also have a principle of mutual assistance between the signatories; however, the mutual assistance principle is only in respect to personnel and does not contemplate critical infrastructure.

[39] Reese, Nick. "The economic case for a Space Critical Infrastructure model." *Space News*, 22 October 2024, https://Spacenews.com/the-economic-case-for-a-Space-critical-infrastructure-model/. Accessed 29 November 2024. See also, for further reading about identifying Space systems as critical infrastructure.

[40] Cilluffo, Frank, et al. "Time to Designate Space Systems as Critical Infrastructure." *University of Auburn*, CSC 2.0, April 2023, https://eng.auburn.edu/mccrary/_files/csc-2-0-report-Space-critical-infrastructure-sector. Accessed 12 December 2024. See for more information about designating Space systems at critical infrastructure and the necessity to safeguard Space systems.

[41] "Space Segment." *GPS*, https://www.gps.gov/systems/gps/Space/. Accessed 11 December 2024.

[42] "Mars Relay Network: Interplanetary Internet." *NASA Science*, https://science.nasa.gov/planetary-science/programs/mars-exploration/mars-relay-network-interplanetary-internet/. Accessed 11 December 2024.

Territorial Claims

States should begin to form international law that governs territorial claims in Space as exploration continues which includes the need for establishing base camps and the possibility of human settlements. In 1984, the UN adopted the Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, "The Moon Agreement." The Moon Agreement states that "The exploration and use of the moon shall be the province of all mankind" in Article IV, and the Agreement emphasizes that the Moon should be used for exclusively peaceful purposes.[43] Outside of this agreement, there is very little international law governing territorial claims for cislunar Space.

International law should be developed to govern territorial claims to prevent conflict resulting from disputed areas of interest. The law should pull principles from The Antarctic Treaty as well as Maritime Law.

The Antarctic Treaty states that Antarctica should be used for peaceful purposes only, there should be freedom of scientific investigation, and scientific findings shall be exchanged freely.[44] The UN treaties largely encompass these principles, but international law should continue to draw upon these principles for areas of Space that may not be physically occupied unlike the surface of the moon. Within this, international law should consider what limitations, if any, states have for installing infrastructure within Space as to not overcrowd cislunar and other layers of Space.

International law should also contemplate maritime law's[45] concept of zones and boundaries. Under maritime law, a state's territorial sea extends 12 nautical miles from its coast, and zones extending past 12 nautical miles are clearly defined in length and use.[46] International law should adopt similar principles for Space. For example, one consideration may include a set parameter around a Space station or other infrastructure that is considered a state's territory. Mitigating the possibility of territorial disputes early will help to keep Space peaceful for all states.

[43] United Nations. "Agreement Governing the Activities of States on the Moon and Other Celestial Bodies." *UNOOSA*, 1984, https://www.unoosa.org/oosa/en/ourwork/Spacelaw/treaties/moon-agreement.html.

[44] The Secretariat of the Antarctic Treaty. "The AntarcticTreaty." Secretariat of the Antarctic Treaty, https://www.ats.aq/e/antarctictreaty.html. Accessed 23 November 2024.

[45] Klein, John J. *Space Warfare: Strategy, Principles and Policy*. p. 47-61. Routledge, 2024. See for more information about concepts that can be borrowed from maritime law to develop Space policies.

[46] National Oceanic and Atmospheric Administration. "Maritime Zones and Boundaries." *National Oceanic and Atmospheric Administration*, https://www.noaa.gov/maritime-zones-and-boundaries. Accessed 3 December 2024.

APPENDIX 2

Cislunar Incident Report Template

Cislunar Incident Report Template

[Organization Name/Watch Center Name]
Incident Report #: [Unique Identifier]
Classification: [e.g., Confidential/Unclassified]
Date and Time of Report: [DD/MM/YYYY HH:MM UTC]

---

1. Executive Summary

- **Incident Title:** [Brief descriptive title, e.g., "Unexpected Orbital Maneuver by Lunar Probe X"]
- **Date and Time of Incident:** [DD/MM/YYYY HH:MM UTC]
- **Location:** [Geographic or orbital coordinates, e.g., "Lunar South Pole, 50 km altitude"]
- **Status:** [Ongoing/Resolved/Under Investigation]
- **Priority Level:** [Low/Medium/High/Critical]

2. Incident Details

- **Description of the Incident:**
  Provide a concise summary of what occurred, including key facts and observations (e.g., "Unplanned trajectory deviation detected for a commercial lunar lander, potential collision risk identified").

- **Source of Detection:**
  [Sensor/network/system that detected the incident, e.g., "cislunar Radar Array XYZ-4 detected anomalous behavior."]

- **Organizations Involved:**
  [List of Spacecraft, operators, agencies, or other stakeholders involved or affected.]

- **Initial Assessment of Impact:**
  [Potential consequences, e.g., "Risk to orbital assets, debris generation, or interference with planned lunar operations."]

3. Critical Systems Impacted

- **Human Life/Life Support** [Description of impacts, current status, assessment]
- **Communications** [Description of impacts, current status, assessment]
- **Propulsion** [Description of impacts, current status, assessment]
- **Guidance** [Description of impacts, current status, assessment]
- **Power/Energy** [Description of impacts, current status, assessment]
- **Habitation** [Description of impacts, current status, assessment]
- **Stakeholders** [Description of impacts, current status, assessment]
- **Disinformation** [Description of impacts, current status, assessment]

4. Actions Taken

- **Timeline of Actions:**
  - [Time HH:MM UTC] Detection of anomaly.
  - [Time HH:MM UTC] Confirmation and validation of data.
  - [Time HH:MM UTC] Stakeholder notifications initiated.
  - [Continue logging major events]

- **Immediate Mitigation Measures:**
  [List any actions taken to address or mitigate the issue, e.g., "Alert issued to Spacecraft operator to execute collision avoidance maneuver."]

5. Current Status

- **Resolution Steps in Progress:**
  [Describe ongoing measures, e.g., "Continued tracking and predictive modeling to monitor risk."]
- **Anticipated Next Steps:**
  [Provide expected future actions, e.g., "Coordination with other operators for additional data analysis."]

6. Preliminary Analysis and Hypothesis

- **Cause (if known):**
  [e.g., "Unplanned engine burn likely caused by onboard system failure."]
- **Potential Contributing Factors:**
  [e.g., "High solar activity may have interfered with guidance systems."]

7. Stakeholder Impacts

- **Affected Parties:**
  [List of stakeholders or regions affected, e.g., "Lunar mining operations by Company A and B in the vicinity."]
- **Communication Measures:**
  [Details of any public statements or stakeholder-specific updates.]

8. Recommendations and Requests

- **Immediate Requests to Stakeholders:**
  [e.g., "Provide telemetry data from Spacecraft involved for further analysis."]
- **Recommended Follow-Up Actions:**
  [e.g., "Conduct systems audit to identify failure points."]

9. Attachments and Supporting Data

- [Include relevant charts, images, or additional data, e.g., orbital paths, sensor readings.]

10. Points of Contact

- **Primary Contact:** [Name, Role, Email, Phone]
- **Backup Contact:** [Name, Role, Email, Phone]