**NASA Security Policies, Governance, and Breaches**



NASA Logo [9]

**Key Contributors:**

**Joseph Drouillard, Briah Graves, Anthony Jamieson**

Text

Description automatically generated

**11/28/2022**

**EXECUTIVE SUMMARY**

The National Aeronautics and Space Administration, abbreviated as NASA, is the USA’s civil space program. The organization works to “explore, discover and expand knowledge for the benefit of humanity” [7]. NASA covers nearly all federal explorations and research into space for the United States and works with many partner companies across the country. Along with research into space, NASA also works towards expansion of programs and technologies to reach space as well as supersonic flight and other related advancements.

This report will cover the security standards, policies, and governance of NASA. To contextualize NASA’s policies and how they operate in the security of the broader organization, the report begins by briefly detailing NASA’s organizational structure, along with its mission, vision, and core values. It then lists select security policies, the roles responsible for security, and processes related to maintaining the integrity of NASA (such as risk management and continuation of operation policies). We then follow up by detailing specific attacks on NASA and their systems, how these attacks circumvented NASA’s defenses, and what strategies they use to mitigate or recover from said attacks.

Since NASA is a prestigious, longstanding federal institution, this report is intended to give a framework by which one can modify or improve their own organization, by learning from, adapting, and modifying the organizational philosophy, governance, and policies of NASA.

Project Milestones:

1. NASA’s Organizational Structure
2. NASA Security Policy and Roles
3. NASA Continuity of Operations
4. Attack History on NASA

Deliverables:

1. Final Report
2. Report Presentation

**PROJECT SCHEDULE MANAGEMENT**

Create a Gantt chart with the application of your choice and replace it with the picture presented below.

Timeline

Description automatically generated with medium confidence

Project Management Board Link (QR Code Only). Send invite to user: @gdparra

Qr code

Description automatically generated

Create a Github Project Repository and add the user “cyberknowledge” as a contributor.

<https://github.com/awjamieson83/NetSecManagementProject>

**TABLE OF CONTENTS**

[**TABLE OF CONTENTS** 4](#_Toc120742010)

[**Milestone 1 – Organizational Structure:** 5](#_Toc120742011)

[NASA Core Values: 5](#_Toc120742012)

[Administrators at NASA: 5](#_Toc120742013)

[Governance Principles: 6](#_Toc120742014)

[**Milestone 2 – Security Policies and Roles:** 7](#_Toc120742015)

[Security Roles: 7](#_Toc120742016)

[Security Exemption: 9](#_Toc120742017)

[Physical Security: 9](#_Toc120742018)

[Security Education, Training, and Awareness (SETA): 10](#_Toc120742019)

[OPS Functional Review: 11](#_Toc120742020)

[Information/cyber security policies: 12](#_Toc120742021)

[Risk Management: 13](#_Toc120742022)

[Risk posture for manned missions: 15](#_Toc120742023)

[**Milestone 3 – Continuity of Operations:** 16](#_Toc120742024)

[Continuity of Operations (COOP) scope: 16](#_Toc120742025)

[Steps for COOP: 17](#_Toc120742026)

[**Milestone 4 – Attack History on NASA:** 19](#_Toc120742027)

[2018 NASA Attack and Related Attacks – JPL Lab at Caltech in Pasadena, California 19](#_Toc120742028)

[1999 NASA Attack 19](#_Toc120742029)

[2006 NASA Attack 19](#_Toc120742030)

[NASA Cybersecurity Readiness Report 20](#_Toc120742031)

[**Professional Accomplishments/Growth Reflection** 21](#_Toc120742032)

[**Difficulty** 21](#_Toc120742033)

[**References** 22](#_Toc120742034)

**Project Milestones:**

# **Milestone 1 – Organizational Structure:**

**NASA Vision: -** “Exploring the secrets of the universe for the benefit of all” [8].

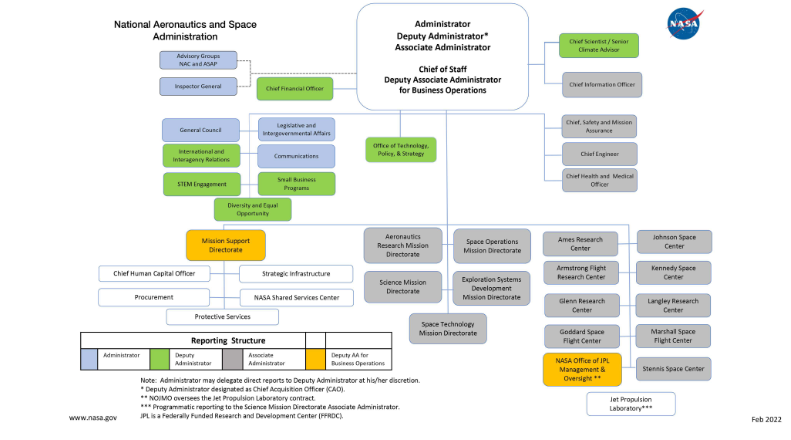
**NASA Mission: -** “NASA explores the unknown in air and space, innovates for the benefit of humanity, and inspires the world through discovery” [8].

## NASA Core Values:

* **Safety**: The well-being of personnel and the public is put above everything else.
* **Integrity**: Ethics are promoted at NASA and built chiefly through trust. One of the most important factors in building trust is allowing for open, candid, respectful communication and critiques from the top down and bottom up.
* **Teamwork**: NASA’s philosophy is that each team member is valuable, as everyone brings a unique perspective to accomplishing the organizational mission, ongoing processes, and solving issues. For this reason, collaboration is heavily encouraged.
* **Excellence**: Every employee is pushed to reach their fullest potential to contribute to the organizational mission [11].

## Administrators at NASA:

* Chief Financial Officer-responsible for tracking cash flow and financial planning and analyzing the company’s financial strengths and weaknesses and proposing strategic directions [20]
* Chief Information Officer-oversees the people, processes and technologies within a company’s IT organization to ensure they deliver outcomes that support the goals of the business [21]
* General Counsel-a company’s main attorney and primary source of legal advice [22]
* STEM Engagement-has developed a series of STEM products and opportunities that provide a platform for students to contribute to NASA’s endeavors in exploration and discovery [23]
* Legislative and Intergovernmental Affairs-provides executive leadership, direction, and coordination of all communications and relationships, both legislative and non-legislative, between NASA and the United States Congress as well as state and local governments [24]
* Communications-provides high-quality, reliable, cost-effective telecommunications systems and services for mission control, science data handling, collaboration, and program administration for NASA programs, projects, and facilities [25]
* International and Interagency Relations-ensures that NASA’s international engagements are in alignment with Administration direction and U.S. laws and regulations [26]



[19] Figure 1: Organizational Chart of NASA

## Governance Principles:

1. Lean governance – NASA utilizes three senior leadership councils to help oversee the organization – EC, PMC, and MSC. The EC oversees NASA’s progress in implementing its organizational vision and helps determine overall strategic missions. The PMC focuses on adjusting mission and program decisions to be in line with NASA’s strategic goals. The MSC deliberates on what processes and assets are needed to ensure the success of planned missions.

2. Clear roles, responsibility, and decision making – Hierarchy, employee power through input, and responsibilities are clearly defined.

3. Strategic acquisition: A variety of acquisition methods are considered when tackling Agency needs, including cooperation with private institutions, reallocating funds, and upgrading assets and infrastructure.

4. Checks and balances – In order to facilitate equanimity within the organization, checks and balances are applied to ensure that no one portion of NASA monopolizes resources or hijacks the organization’s mission focus. Checks and balances are also used to ensure that the open exchange of ideas and suggestions can flow freely, preventing stagnation. For example, peer (lower level) reviews and oversight (higher level) reviews are both taken into consideration by management; organizational programs are reviewed by unaffiliated employees to determine the progress and merit of the mission; and personnel are able to raise dissenting opinions over project or even institutional direction without fear of reprisal, so long as said opinions are supportable and aren’t of a trivial nature [11].

# **Milestone 2 – Security Policies and Roles:**

**Security Standards and Laws:** In the pursuit of information security, NASA follows the protocols given by NIST Special Publication 800 series, as well as the NIST Federal Information Processing Standards [13]. In risk management, the processes of RIDM and CRM must conform to NPD 1440.6 and NPR 1441.1 [18]. NASA’s Office of Protective Services verifies that NASA’s COOP conforms to a special version of the Federal Emergency Management Agency Federal Continuity Evaluation Tool [15]. The existence of a comprehensive COOP for NASA (covering the protection of the mission, key assets, operation continuation, and information systems) is mandated by federal legislation EO 12656 (Assignment of Emergency Preparedness Responsibilities); HSPD-7; NSPD 51 (National Continuity Policy); Computer Security Act of 1987; and OMB circular A-130 [15].

## Security Roles:

NASA Centers are semi-independent locations that operate within the NASA Agency. While there is a level of agency in the security and management policies each Center can implement, there are also several agency-wide and federally enforced policies each must conform to. [16]

All Centers have security compliance put into practice by a Center Director of Protective Services (CCPS) and Chief of Security (CCS). The Office of Protective Services (OPS) verifies that all of NASA’s centers adhere to agency-wide security policies and standards [16].

Resource provision in the advancement of security is given by the Assistant Administrator for the Office of Protective Services (AA, OPS) [16; 12]. AA, OPS also helps define best practices for the agency, identify vulnerable infrastructure points, and manage the Enterprise Risk Management Program. Any reports of espionage, sabotage, on-premises strikes/protests, weapon discharges, and suspicious network activity are to be forwarded to and handled by the AA, OPS [16]. AA, OPS also has the power to revoke personnel clearances, and acts as NASA’s chief representative when communicating with national intelligence organizations [12].

OPS is responsible for making an Insider Threat program in preparation for malicious actions from employees or contractors and is also responsible for background checks and validating the qualifications of NASA security personnel [12].

Centers have leaders called Center Directors. They can elect to build upon the agency-imposed security policies within their center [16]. Center Directors also work to enforce the organization’s infosec policy within their respective Center, and are ultimately held responsible for the confidentiality, integrity, and availability of information and information assets within their area of governance [13]. In the context of risk management, Center Directors must handle institutional risks [18]. If a manned mission is being undertaken under a Center Director’s jurisdiction, the Center Director has the authority to stop the mission [14. Center Directors ensure that the center’s security program is reviewed periodically, report suspected espionage and terror attempts on center grounds to the NASA Counterintelligence/Counterterrorism office. They can also revoke the clearance of security personnel in the center [12]. Center Directors must also designate Center COOP coordinators, verify that the Center Chief Financial Officer allocates appropriate resources towards COOP functionality, and cements COOP as part of the Center’s mission [15].

Supervisors, program managers, and line managers are responsible for verifying that security policies within their respective programs are adhered to and have the power to revoke the clearance of personnel under them [16]. Program and project managers also must handle risk within their ongoing projects [18]. Program and project managers determine mission and safety objectives for manned crews’ objectives; act if a risk is deemed too dangerous for assets, personnel, or the public; and work with the Office of International and Interagency Relations to share information about mission risk with appropriate organizations and entities, such as foreign organizations and governments [14].

The NASA Administrator is tasked with risk assessment of information and information system assets, putting risk management policies into practice, and verifying that infosec security management is inseparable from NASA’s regular operational planning [13]. Administrators also approve risk levels for NASA’s space crew personnel and help to foster a culture of safety within NASA [14]. The Agency COOP coordinator is also selected by the Administrator [15].

Mission Directorate Associate Administrators (MDAAs) determine risk acceptance levels for manned missions within their jurisdiction; monitor the progress of risk management in their crewed missions; and act if a risk is deemed too dangerous for assets, personnel, or the public [14].

All employees and visitors to NASA centers and sites are held culpable for security adherence [16].

NASA’s CIO ensures that information security policies are followed, determines cybersecurity policies (with the help of the Assistant Administrator for OPS) and disseminates infosec security awareness materials, verifies that procedures exist for reporting and investigating infosec incidents, and employs governance groups to help ensure that information security policies are observed [13].

NASA’s CISO helps the CIO in ensuring compliance with NASA’s infosec policy, in part by allocating resources to NASA Centers. The CISO also refers sufficiently serious infosec incidents to various senior personnel, such as the NASA Counterintelligence Director or the NASA OIG [13].

Mission directorates are responsible for managing programmatic and technical risks at the domain level [18].

The Agency COOP is charged with ensuring that COOP is integrated into NASA’s mission. This is achieved through making a COOP Multiyear Strategy and Program Management Plan, and by working closely with Center COOP coordinators to ensure proper COOP modifications and additions for different locations. The Agency COOP coordinator is also responsible for managing COOP documentation as per NPD 1440.6 and for organizing Agency-wide training and tests [15].

Center COOP coordinators are charged with leading the formulation of center COOPs in line with required agency and Center policy; working with the Agency COOP coordination to plan annual COOP training and tests; and coordinating tenant organization COOP development [15].

## Security Exemption:

Any NASA Centers which find themselves in violation of Agency wide security policies are allowed to file a petition for a temporary exemption of up to a year to get back up to regulation [16].

## Physical Security:

Each NASA center must have access control points (ACPs) through which traffic is to be funneled. These are established to dissuade intrusion and allow security to validate the identity of purported personnel attempting to enter the Center. Identity validation is performed by Security Police Officers, who check photographs and authentication cards. Security Police Officers are also charged with responding to onsite disturbances [16].

ACPs which lead to particularly sensitive or vulnerable areas may have additional security measures beyond Security Police Officer checkpoints, such as electronic access equipment and security barriers [16].

Any visitor to a NASA center may have their person or possessions searched by authorized NASA personnel at any time. All NASA visitors consent to this since all legitimate entrances to the NASA Center contain signs detailing this policy. The CCPS, CCS, and Center Director all have the right to expel any employees or visitors from the premises under suspicion of malicious intent; if the offender is an employee, expulsion will be preceded by a revocation of access privileges and confiscation of authentication cards. In the case of an ongoing terror attack on NASA premises, the AA, OPS is also charged with raising the alert level and initiating conversation with the FBI and DHS [16].

Any public protests taking place by NASA centers are to be redirected off center grounds, unless approved for entry by the Center OCC/OGC. In the event of such protests, the CCPS/CCS must ensure that the demonstration remains orderly and safe, that NASA assets and information are not harmed, and that all personnel dealing with the protestors have proper training [16].

NASA divides security areas into three types: NASA controlled area, NASA limited area, and NASA exclusion area. All three of these areas are closed to the public except in cases of special exemptions, in which case the visitor is to be always escorted [16].

A NASA-controlled area and limited area are similar in their functions as designated zones to segregate information, equipment, and sensitive work environments from the public or unauthorized employees. The main difference between them is that NASA-limited areas usually employ more stringent physical security measures, such as barriers and (unspecified) access denial equipment. A NASA exclusion area is used for storing Classified National Security Information (CNSI) [16].

Additionally, whereas one must complete appropriate training to enter a controlled area, entry to a Limited and Exclusion Area must see the employee escorted unless they have the appropriate security clearance and must access the area’s assets or information to accomplish their duties [16].

The CCPS/CCS has liberty to implement additional security measures to the Limited and exclusion areas beyond what is specified in the NPR [16].

All NASA locations (Centers, Headquarters, Laboratories, etc.) must document and forward statistics on on-premises criminal incidents, security clearance grants and revocations, positive developments of note, and security violations every three months [12].

## Security Education, Training, and Awareness (SETA):

Center Director ensures that all personnel in the center are aware of their duties as per the security program. The CCPS/CCS puts this into practice by applying security training for appropriate personnel in coordination with NASA supervisors.

Among the necessary trainings are:

1. Initial Orientation Security Briefing – This sees new employees educated on basic security obligations and tenets, including but not limited to: entry and exit control procedures, the importance of security credentials, how to handle Personally Identifiable Information, and how and when to report suspicious activity.

2. Annual Security Training – Used to ensure that employees do not disregard or forget what was taught in Initial Orientation.

3. Supervisory Security Training – Specialized security briefing given to new employees based on their roles.

4. Security Clearance Briefing – Given to employees about to receive some level of security clearance. Includes (but not limited to) how and when to use Need-to-Know to access confidential information, how to handle CNSI, and the employee’s responsibility in reporting suspicious behavior from other clearance holders.

5. Annual Security Clearance Refresher Briefing – Used to ensure that clearance holding personnel do not disregard or forget what was taught in the first Security Clearance Briefing.

6. CNSI Custodian Briefings – Annual briefings on the duties of those responsible for maintaining CNSI records, or the facilities/assets containing said records.

7. CNSI Termination Briefing – Briefings given to personnel whose access to CNSI was revoked. Reminds the personnel that their obligation to confidentiality of CNSI is binding even in the case of retirement, termination, or transfer, and that penalties will be applied if said confidentiality is breached [16].

## OPS Functional Review:

The OPS Functional Review is a review of security policies at NASA Centers. It is meant to ensure that security policies are in compliance with federal and NASA standards. This review must be carried out at once every three years [16].

**Policies concerning the transfer of NASA information and assets outside the US**:

If any NASA personnel must travel outside the US for business, they shall take only as much confidential information with them as is needed for the execution of their duties, be the information physical or digital. This applies also to NASA assets such as work computers. All such devices must be approved by the CIO’s office for use in travel, and confidential NASA information may *only* reside on these approved devices. Detachable media storage devices used at events must not be reentered into the organizational device. The workstation must not be connected to any other device and must be in airplane mode while not in use. The workstation must not be used for recreation, cannot be used to download from App Stores, and must not be shared with friends, relatives, or strangers [17].

Any information taken with the employee must be backed up with the help of the CIO’s office before departure [17].

If any information or assets are compromised during travel, the employee must immediately report the incident to NASA Security Operations Center (SOC) [17].

While traveling, employees may only access NASA confidential information and domains through their designated NASA device [17].

NASA employees are not allowed to bring organizational assets or information with them on leisure travel. If a need for such materials arises while outside the US, the employee must receive permission from their supervisor to have a NASA device delivered to them with the help of their Center’s OCIO [17].

## Information/cyber security policies:

**Information incident reporting:**

In the case of any incidents involving the compromise of information or the failure of information system assets, NASA mandates that an after-action report is developed for documentation purposes and to critique any deficiencies in the mitigation and response process [13].

**Software policy**:

Any third-party software to be used within NASA must be determined safe before its operation is approved [13].

**Network monitoring**:

While no comprehensive document dedicated to agency-wide network monitoring could be found, a document on this policy was found for one of NASA’s Centers, the Armstrong Center. Its details are given below:

IT Security personnel and the Office of the CIO (OCIO) are charged with monitoring Armstrong Center network traffic, including IP addresses, protocols, ports, and specific content. These personnel are allowed to deploy intrusion detection systems or (where it is practical or necessary) manually examine packets or content. Verified IT personnel and OCIOs are responsible for managing collected network and IDS logs. If potentially malicious activity is detected, IT personnel and the OCIO inform the Center’s CISO, who does additional analysis [10].

The Center Chief Information Officer vets all new testing procedures concerning the Center’s networks, and keeps the Center Director apprised of any noteworthy, potentially malicious activity [10].

If any anomalous activity is bookmarked by IT personnel or the OCIO, the Center Information Security Officer performs a thorough inspection and makes the decision on how to proceed. If it is determined that the traffic is suspect, the policies listed in NPR 2800.2, NPR 2810.1, NPD 2810.1, and NPR 2841.1 will be consulted [10].

## Risk Management:

**Risk management policy**:

NASA is particularly concerned with risk that affects these key domains of interest (though other domains may be affected as well):

1. Safety

2. Mission success

3. Physical security and cybersecurity

4. Cost

5. Schedule [18]

NASA represents risk via three qualities:

1. The specific scenario engendering compromised information, infrastructure, assets, safety, and/or schedule delays.

2. Likelihood of said scenario’s occurrence.

3. A quantitative or qualitative measure of how severe each scenario’s successful execution would be [18].

NASA’s risk management process is composed of two operations: Risk-Informed Decision Making (RIDM) and Continuous Risk Management (CRM) [18].

The process of RIDM is intended to determine how to best meet performance requirements, and it involves three steps:

1. Identification of alternatives – Risks are documented; objectives and performance measures are defined; decision alternatives are made and documented.

2. Analysis of Alternatives – Decision alternatives are analyzed for merit.

3. Risk-Informed Alternative Selection: One of the decision alternatives is adopted; the decision and justification are recorded, along with pros and cons of the decision [18].

CRM is meant to manage risks, and it has six steps:

1. Identify – Identify what factors contribute to risk.

2. Analyze – Calculate probability and impact of the risk.

3. Plan – Formulate mitigation and contingency plans, risk handling, and risk tracking.

4. Track – Carefully log variables indicative of ongoing attacks (such as abnormal logs, sudden network traffic spikes, etc.).

5. Control – Analyze and compare tracking data to verify if mitigation plans are sufficient or require correction.

6. Communicate and Document – Maintain and update detailed documents of the other 5 steps of the CRM process [18].

Note: If risk management is transferred from a lower organizational unit to a higher one, thresholds, impact, probability, and other considerations for the risk must be recalculated in the context of the new organizational unit [18].

CRM and RIDM are complementary and executed in each organizational unit [18].

The Risk Management Plan (RMP) proper must lay out risk tolerance for the organizational unit it applies to; take into account all applicable risks for the organizational unit; formulate how the organizational unit will apply RIDM and CRM; describe the process for measuring likelihood and severity of each risk; concretely define risk acceptance measurements; ensure proper coordination with risk management plans from other organizational units; identify stakeholders involved with the risk management process; create agreed upon protocols for different management levels to communicate with one another about risk; track decisions on accepting risk thresholds via documentation; decide upon a time frame for when to conduct risk acceptance decision reviews; ensure that RIDM and CRM conform to NPD 1440.6 and NPR 1441.1 [18].

There are six decisions to be made regarding dealing with risk:

1. ACCEPT – The risk is accepted as is. This acceptance and its justification are documented and periodically reviewed in case the rationale for the acceptance decision is obsolete.

2. MITIGATE – The risk is mitigated, and the risk mitigation plan is created and documented.

3. CLOSE – The risk is determined to no longer be an active concern and is closed; after upper management approves this decision, the decision and its justification are both documented.

4. WATCH – The risk is monitored closely, with no other actions taken. Tracking requirements are documented.

5. RESEARCH – If none of the four previous decisions seem to apply, the risk is researched so that new information might point to the proper course of action. The research process is documented.

6. ELEVATE – If research yielded inconclusive results, the risk is instead elevated to a higher organizational management unit for their input [18].

To maintain proper historical documentation and help decide on current and future risk management decisions, the risk management implementation process, effects of risk management decisions, the rationale for risk acceptance decisions, and data related to risk management decisions’ efficacy are all tracked [18].

## Risk posture for manned missions:

When defining missions and the missions’ execution, space and aircrew must have a defined risk posture and take into account the repercussions of mission failure, including potential risks to assets, personnel, and the general public. All identified risks in such manned missions must be sufficiently mitigated and/or accepted before the crews’ assignment begins. This is accomplished through the implementation of best practices, thorough training, safety regulations and standards, and external consultations where appropriate. Supervisors and crew personnel have the explicit right to object to missions they deem too dangerous, without fear of retaliation from upper management [14].

NASA prioritizes flexibility in adapting to sudden developments on missions and in documenting mission data (both positive and negative) for future mission plans and implementation [14].

# **Milestone 3 – Continuity of Operations:**

## Continuity of Operations (COOP) scope:

NASA Continuity of Operations applies to supporting facilities, IT systems, operations central to the organization’s missions, and other assets/proceedings vital to the Center and agency wide performance of NASA [15].

NASA defines the goal of COOP as:

1. Allowing operations essential to the organizational mission to continue in the case of unforeseen or sudden incidents.

2. Defending NASA assets, records, and equipment.

3. Mitigate impediments to major operations.

4. Protect life (of employees and the public).

5. Bring possible danger to an acceptable level.

6. Lay the path for normal operations to resume in a reasonable time frame [15].

**Characteristics of a successful COOP state:**

NASA maintains that COOP is only in an acceptable state if:

1. It can be put into practice on little to no warning

2. It can be maintained at a high readiness level

3. It can take full effect within a maximum of 12 hours of initial activation

4. It can maintain mandatory organizational operations for at least 30 consecutive days

5. It takes *all* potentially helpful infrastructure, assets, plans and procedures into account [15].

**Judgements for COOP**:

To support the COOP process, NASA centers must ensure that they have sufficient, functional Agency Mission Essential Infrastructure (MEI) supporting operations.

When making judgements for COOP, Center staff must take the following points into consideration:

1. Will the compromise of a Center MEI endanger national security?

2. Will the compromise of Center MEI endanger the public?

3. Is this center’s MEI or operation depended upon by another Center or agency’s COOP, and is there a binding agreement that the latter’s COOP must remain functional?

4. Is the Center’s contribution to NASA’s mission mandatory to remain functional at all costs by executive order?

5. Is the MEI in question space exploration equipment or a vital component of the exploration mission? If so, would its compromise affect personnel or vital asset safety? And how severe would the financial cost of such an event be?

6. Does the operation being analyzed fall under the umbrella of COOP by NASA management’s definition (a vital service for the agency’s mission) [15]?

## Steps for COOP:

The major steps of the Continuity of Operations Planning Process are:

1. The organization’s MEI operations are analyzed in the lens of the business plan.

2. An order of priorities is established for business processes.

3. The Program Manager validates the completion of the business plan’s analysis.

4. The least vital functions which are economically unfeasible to fully support in the context of COOP are deprioritized.

5. The organizational unit’s operations are compared to the Agency’s mission statement to determine what operations are necessary for the continuation of NASA’s mission. Interorganizational dependencies between operations and their assets are also taken into account and documented.

6. Criticality matrix is developed with the aim of quantifying the criticality of an organizational unit’s operations.

7. All vital resources for the organization’s mission are accounted for and documented, alongside their timeframes of use. Some examples of some categories of resources include human resources, IT-Based Services, automated applications and data, secure communications, and physical infrastructure.

8. Delegations of Authority (DOA) are made at NASA locations. This streamline decision making so that vital decisions in the middle of an incident aren’t slowed unnecessarily by bureaucracy.

9. Plans of Succession (POS) are established for key personnel in case they are unavailable or incapacitated, and their duties must be carried out by another.

10. As wide an area of addressable threats as possible are documented.

11. Specific COOP strategies are chosen, bearing in mind the five main components of a COOP strategy: prevention (the technique for preventing or at least delaying a disaster); active response to the disaster; resumption (the process of allowing operations to continue before complete recovery); recovery (other processes beyond those most highly prioritized by COOP are reactivated); restoration (a return to the status quo).

12. Plan to cross train or temporarily hire outsourced employees in case the disaster somehow causes a shortage of staff.

13. Maintain IT operations with a choice of a hot site, cold site, redundant site (an exact copy of the original site), reciprocal agreement with a separate private or federal organization, or a hybrid of one or more of the aforementioned choices.

14. There must be a plan in place to backup data in case of a disaster. Electronic files must be backed up weekly. Both master copies and copies of paper documentation are to be stored offsite.

15. Adequate communication alternatives must be ready in case of a disaster; this can include functional communication at alternative work sites, or a separate layer of contingency communication.

16. Plans must be in place for what physical equipment to move in case the need arises for rapid redeployment of physical assets to or from an alternative site.

17. Physical documentation copies should be cycled on a timetable determined by management’s higher ups. Storage offsite or near (but not directly in) the primary site is also recommended.

18. Document the COOP. Ensure that it is regularly updated, able to be accessed in case of a disaster, is easy to follow and implement in case regular professionals are unavailable, and is stored redundantly. The sections of the COOP are:

(a) Plan overview – An overview of the scope, roles, and objectives.

(b) Continuity process overview – Describe the latter four COOP stages (active response to the disaster, resumption, recovery, and restoration).

(c) Continuity team organization – Overview of the teams and their designated tasks meant to accomplish the COOP.

(d) Plan maintenance - Details the timetables and goals of plan review, in case the COOP needs alterations in lieu of new threats or organizational developments.

(e) Plan exercise – Documents the types of tests to be performed on the existing COOP process – this is expected to happen at least once a year.

(f) Plan execution – Instructions on how to execute the COOP plan – include references to upper management who must be informed of an onsite disaster, the tasks of each team, where important information is backed up, the existence of alternative sites, etc.

19. Test and revise strategy – COOP is tested for several possible reasons:

(a) Review – The information and methods within the COOP plan are reevaluated, such as whether backup sites or contact information is up to date.

(b) Analysis – The COOP plan is exercised, in part or whole, in order to find any potential weaknesses.

(c) Simulation and test – A recreation of the COOP plan in real time by at least one team, in order to find potential pitfalls in the COOP and to ensure that teams are ready in case the need for the COOP plan arises [15].

# **Milestone 4 – Attack History on NASA:**

## 2018 NASA Attack and Related Attacks – JPL Lab at Caltech in Pasadena, California

One of NASA’s hotspots for cyberattacks is their Jet Propulsion Lab in Pasadena, California at Caltech. In April 2018, an unauthorized Raspberry Pi gained access to the JPL servers [1]. The hacker moved laterally throughout the NASA systems, such as the Deep Space Network radio telescopes and other systems hosted at NASA Jet Propulsion Laboratory. This attack made the Johnson Space Center disconnect from JPL’s gateway in fear that the attacker may move into mission systems and commit malicious activities toward human space flight missions [1].

With this known, an audit report was released by the NASA Office of the Inspector General that covered this incident and many other related attacks that occurred at NASA JPL. One notable attack listed is one that happened in January 2009 where an attacker stole 22 gigabytes of program data and transferred it to an IP address that resided in China [2]. This is just one of many examples showing how the information held by NASA is often invaluable to nation-state threat actors who stand to gain from confidential research and documents. Five other similarly intrusive attacks are listed after, showing the lack of proper security in the lab. From these exploits, the NASA OIG goes on to list many of the faults they found inside the JPL’s security controls, such as inadequate system inventories, improper network segmentation, untimely security log ticket resolution and system patching, and broken log management infrastructure to name a few. After the conclusion of the OIG’s findings, a ten-point recommendation and evaluation was made on how to further remediate the issues outlined in the audit report.

## 1999 NASA Attack

Another high-profile incident occurred back in 1999 when a 15-year-old boy hacked into DoD computers. Between August and October, the hacker, Jonathan James, accessed the computers of the Defense Threat Reduction Agency (DTRA) [3]. Using collected credentials, he made use of privilege-escalation attacks to gain access into other government systems, such as the systems of NASA’s Marshall Space Flight center. On one of the systems, James found source code for critical modules of the International Space Station. As soon as NASA was aware of the attack, they began an internal investigation that lasted three weeks and cost NASA around 40,000 dollars [3].

## 2006 NASA Attack

In 2006, over 150 government computers were broken into by a 26-year-old Romanian man named Victor Faur [4]. After the FBI alerted Romanian police, they arrested Faur who the police had stated had previously hacked into computer systems of US universities as well as government agencies, including NASA. The two facilities from NASA that had been accessed were the Goddard Space Center and the Jet Propulsion Lab [5]. Though Faur tried to state in interviews that he had not tried to steal information from these agencies and was simply proving that many computers were vulnerable to cyberattacks, NASA could not rely on data from the hacked systems and had to manually rebuild them [4]. This attack cost NASA around 1.4 million dollars to remediate.

## NASA Cybersecurity Readiness Report

In a 2021 Cybersecurity Readiness Report posted by the NASA Office of Inspector General, NASA reflects on the company’s readiness to defend against different threats in a growingly hostile cyberspace environment. In the report, the OIG states that in the previous four years “NASA experienced more than 6,000 cyber-attacks, including phishing scams and introduction of malware into Agency systems” [6]. The authors continue to explain that because NASA is a government entity, performs high-profile missions, and carries large amounts of often sensitive data, they are a regular target for cyberattacks. For 2020 alone, the OIG also states that NASA identified 1,785 cyber incidents.

# **Professional Accomplishments/Growth Reflection**

1. Learned more about the governance philosophies and principles that shape successful organizations – including the promotion of constructive conversation between employees and management, flexibility in crisis response and governance, and a commitment to employee well-being.
2. Saw a limited degree of the real-life applications of security policies/measures on a large, successful organization.

# **Difficulty**

1. Some of the policies, or their specifics, were hidden from public view.
2. It was difficult at times to choose and sort through what information to cover in the paper.
3. Organization of the report structure seemed to be challenging with the amount of information we wanted to convey.

# **References**

Winder, D. (2021, June 30). *Confirmed: NASA has been hacked*. Forbes. Retrieved from https://www.forbes.com/sites/daveywinder/2019/06/20/confirmed-nasa-has-been-hacked/?sh=370541a9dc62[1]

Martin, P. K., Tolomeo, R., Saucedo, G., Bennett, J., Doan, A., Geranmeyeh, C., Liu, J. Y., Sedighi, B., & Suls, L. (2019, June 18). *CYBERSECURITY MANAGEMENT AND OVERSIGHT AT THE JET PROPULSION LABORATORY*. NASA Office of Inspector General. Retrieved 2022, from https://oig.nasa.gov/docs/IG-19-022.pdf[2]

Petkauskas, V. (2022, September 17). *How a Florida teenager hacked NASA’s source code*. Cybernews. Retrieved 2022, from https://cybernews.com/editorial/how-a-florida-teenager-hacked-nasas-source-code/[3]

New Scientist, & Afp. (2006, December 4). *Hacker charged for breaching NASA Computers*. New Scientist. Retrieved 2022, from https://www.newscientist.com/article/dn10723-hacker-charged-for-breaching-nasa-computers/[4]

Gradijan, D. (2006, December 1). *Romanian man indicted for hacking into U.S. govt. computers*. CSO Online. Retrieved 2022, from https://www.csoonline.com/article/2120882/romanian-man-indicted-for-hacking-into-u-s--govt--computers.html[5]

Martin, P. K., Colon, T., Riggenbach, S., Hargrove, L., & Reeves, C. (2021, May 18). *NASA’S CYBERSECURITY READINESS*. Oversight.gov. Retrieved 2022, from https://www.oversight.gov/sites/default/files/oig-reports/NASA/IG-21-019.pdf[6]

Loff, S. (2015, January 28). *About NASA*. NASA. Retrieved 2022, from https://www.nasa.gov/about/index.html [7]

Blodgett, R. (2018, April 20). *Our Missions and Values*. NASA. Retrieved October 15, 2022, from <https://www.nasa.gov/careers/our-mission-and-values> [8]

Wikimedia Commons. (n.d.). *Nasa logo*. Wikimedia Commons. Retrieved November 28, 2022, from <https://commons.wikimedia.org/wiki/File:NASA_logo.svg>. [9]

NASA. (n.d.). *AFPD-2810.1-001, Baseline-8*. Retrieved November 25, 2022, from <https://www.nasa.gov/sites/default/files/atoms/files/afpd-2810.1-001_0.pdf> [10]

NASA. (n.d.). *NPD 1000.0B*. Retrieved November 26, 2022, from <https://nodis3.gsfc.nasa.gov/NPR_attachments/N_PD_1000_000B_.pdf> [11]

NASA. (n.d.). *NPD 1600.2E*. NASA. Retrieved November 25, 2022, from <https://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PD_1600_002E_&page_name=main&search_term=information+security> [12]

NASA. (n.d.). *NPD 2810.1F*. Retrieved November 24, 2022, from <https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPD&c=2810&s=1E> [13]

NASA. (n.d.). *NPD 8700.1F*. NASA. Retrieved November 24, 2022, from <https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPD&c=8700&s=1F> [14]

NASA. (n.d.). *NPR 1040.1*. Retrieved November 27, 2022, from <https://nodis3.gsfc.nasa.gov/npg_img/N_PR_1040_0001_/N_PR_1040_0001_.pdf> [15]

NASA. (n.d.). *NPR 1600.1a*. NASA. Retrieved November 24, 2022, from <https://nodis3.gsfc.nasa.gov/npg_img/N_PR_1600_001A_/N_PR_1600_001A_.pdf> [16]

NASA. (n.d.). *NPR 2810.2*. Retrieved November 25, 2022, from <https://nodis3.gsfc.nasa.gov/npg_img/N_PR_2810_0002_/N_PR_2810_0002_.pdf> [17]

NASA. (n.d.). *NPR 8000.4C*. Retrieved November 24, 2022, from <https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=8000&s=4A> [18]

NASA. (n.d.). *Nasa Organizational Chart (Feb. 25, 2022)*. NASA. Retrieved November 30, 2022, from <https://www.nasa.gov/sites/default/files/atoms/files/nasa_organization_chart_feb-25-2022.pdf>. [19]

Dunbar, Brian. “Jeff Dewit, Chief Financial Officer.” *NASA*, NASA, 3 Apr. 2018, <https://www.nasa.gov/feature/jeff-dewit-chief-financial-officer/#:~:text=Jeff%20DeWit%20was%20unanimously%20confirmed%20by%20the%20U.S.,resources%20toward%20the%20achievement%20of%20NASA%27s%20strategic%20plan>. [20]

Dunbar, Brian. “Office of the Chief Information Officer.” *NASA*, NASA, <https://www.nasa.gov/offices/ocio/home/cio_home_insert.html#:~:text=The%20NASA%20CIO%2C%20as%20the%20Agency%27s%20change%20agent,Agency%20achieves%20an%20acceptable%20return%20on%20its%20investment>. [21]

Burns, Laura. “About the Office of the General Counsel.” *NASA*, NASA, 28 July 2015, <https://www.nasa.gov/offices/ogc/about/index.html>. [22]

May, Sandra. “Stem Engagement at NASA.” *NASA*, NASA, 13 Mar. 2018, <https://www.nasa.gov/stem/about.html>. [23]

Dollar, Andrew. “Welcome.” *NASA*, NASA, 30 Mar. 2015, <https://www.nasa.gov/offices/olia/home/index.html>. [24]

Porterfield, Michael. “Communications.” *NASA*, NASA, 26 July 2016, <https://www.nasa.gov/content/communications>. [25]

Shea, Garrett. “NASA's Office of International and Interagency Relations (OIIR).” *NASA*, NASA, 7 Dec. 2017, <https://www.nasa.gov/oiir/home>. [26]