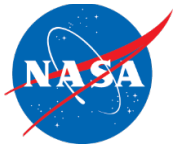
National Aeronautics and
Space Administration

Mary W. Jackson NASA Headquarters
Washington, DC 20546-0001



GUI 1058.2
NPR 1058.1

January 4, 2022

Reply to Attn of: Enterprise Protection Program

TO: Associate Administrator for Aeronautics Research Mission Directorate
Associate Administrator for Exploration Systems Development Mission Directorate
Associate Administrator for International and Interagency Relations
Associate Administrator for Mission Support Directorate
Associate Administrator for Science Mission Directorate
Associate Administrator for Space Operations Mission Directorate
Associate Administrator for Space Technology Mission Directorate
Chief Engineer
Chief Information Officer
Chief, Safety and Mission Assurance
Assistant Administrator for Human Capital Management
Assistant Administrator for Protective Services
Assistant Administrator for Strategic Infrastructure
Center Directors

FROM: Principal Advisor for Enterprise Protection

SUBJECT: Security Clearance Best Practices

Background

Protection of NASA's space and aeronautical systems, corporate systems, and infrastructure systems relies upon Classified National Security Information to understand malicious threats or risks to those systems. In some cases, information necessary to mitigate those threats or risks also is classified.

The Enterprise Protection Program NPR 1058.1 recognizes the use and importance of Classified National Security Information for Agency protection:

1.2.3 The [Principal Advisor for Enterprise Protection] PAEP and [Enterprise Protection Program] EPP will use threat information, including classified threat information, and insight into system protection activities of Mission Directorates and Offices to integrate system protection work across the Agency. This information and insight will inform the work and recommendations of the PAEP and EPP to ensure resilience of the enterprise.

1.2.8 Much of the work of the PAEP and EPP involves the use of classified threat and technical information. As a result, the PAEP and NASA EPP representatives from Mission Directorates, Offices, and Centers shall hold Top Secret/Sensitive Compartmented Information clearances.

When a position is established, NASA uses the OPM Position Designation Tool (PDT) which is included in our electronic position descriptions (PD) system built on Government-wide standards. In December 2018, NASA completed a comprehensive review of all PDs to ensure that the appropriate levels of risk and sensitivity (i.e., national security clearance levels) were established for each position. The review was coordinated among the Office of the Chief Human Capital Officer (OCHCO), the Office of Protective Services (OPS), and NASA supervisors. NASA has initiated the security clearance investigation process for all positions that resulted in an upgraded risk designation.

To ensure that an issue does not occur because personnel lack the appropriate clearance levels, internal reviews will be conducted annually on a random sampling of positions and all positions will be reviewed every three years.

Objective

The objective of this memo is to identify best practices and recommendations regarding positions relating to flight program development and operations that should be designated for a security clearance. Such clearances enable:

a. Awareness of threats and risks to flight programs from malicious actions.

b. Awareness of mitigation strategies to enable decisions to be made on how to protect flight programs.

The policies of OCHCO and OPS, the OPM PDT, and determinations by representatives of OCHCO, OPS, and NASA supervisors take precedence over this guidance.

This guidance is focused primarily on civil service and JPL positions that directly manage flight programs or provide technical oversight of flight programs and is not intended to cover all aspects of Agency operations.

David E. Adams

David E. Adams

Enclosures:
1. Best Practices for Security Clearances for Flight Programs/Projects
2. Matrix of Recommended Security Levels for Positions Relating to Flight Program/Project Development and Operations
3. Change Log

Best Practices for Security Clearances for Flight Programs/Projects

Best Practice #1

Background

Occasionally, threat or vulnerability information is received relating to an aspect of NASA flight programs or operations. This can be in the form of a type of threat to a spacecraft, or a threat to information systems (i.e., cybersecurity threat). If this threat or vulnerability information is classified, then information can only be shared with personnel holding a requisite clearance and need-to-know. However, this information can be of an urgent nature for operational or other reasons and must be addressed with personnel who hold a lower clearance or no clearance. The best practice described below provides two options that could be pursued in such cases.

Best Practice

- Downgrading of Information: When necessary, the Headquarters (HQ) Office of Protective Services Intelligence Division can seek a downgrading of a subset of the classified information to a lower level of classification. This would then allow that downgraded subset to be provided to personnel who hold a lower clearance and need-to-know. Because downgrading can take weeks or months to accomplish, having cleared personnel in place remains important.

- Interim SECRET Clearance: When necessary, the HQ OPS or Center OPS, could grant an interim SECRET clearance to enable SECRET level information, to be provided to personnel with the necessary need-to-know. In this case, the Position Description of the personnel must first reflect the need for such information.

Best Practice #2

Background

It can take two or more years to be granted a security clearance at the Top Secret/Sensitive Compartmentalized Information (TS/SCI) level. Many engineering subsystems are subject to malicious threats or risks, such as Radio Frequency (RF) jamming or spoofing of communication links for Position, Navigation, and Time (PNT) services. Many subsystem engineers go on to become mission systems engineers, a position for which a TS/SCI security clearance is highly desirable.

Best Practice

For an engineering position involving a subsystem subject to malicious threats or risks, for which access to Classified National Security Information is needed to understand the threat, risks, or mitigations, NASA supervisors should consider this factor in the determination of clearance requirement for the position.

Best Practice #3

Background
In many cases, the guidance above leads to personnel having a clearance, but the administrative supervisory chain not having a similar clearance. This situation is acceptable and is consistent with principles of need-to-know for information security.

Best Practice
In situations where a supervisor does not have comparable clearance levels compared to employees supervised, supervisors are encouraged to delegate to a functional lead who is cleared to the required level.

Best Practice #4

Background
In many cases, new flight projects are established through an open competitive process, leading to project management being comprised of non-civil servants. Currently, such project management is not required to have or obtain a security clearance.

Best Practice
In cases of non-civil servant project personnel, use of Trusted Agents from the managing Center is a way to enable the Project Protection Plan to be as comprehensive as possible for the mitigation of risks arising from malicious threats.

Matrix of Recommended Security Levels for Positions Relating to Flight Program/Project Development and Operations

Headquarters

Position	Recommendation
Mission Directorate AA	TS/SCI
Mission Directorate Deputy AA	TS/SCI
Mission Directorate Flight Programs Deputy AA, or Division Directors with flight program management responsibilities	TS/SCI
Mission Directorate personnel supporting Enterprise Protection Note: These personnel may serve as Trusted Agents and support other Mission Directorate personnel (e.g., Program Executives) on Enterprise Protection matters.	TS/SCI

Centers

Position	Recommendation
Center personnel supporting Enterprise Protection Note: These personnel may serve as Trusted Agents and support other Center personnel (e.g., Program or Project Managers) on Enterprise Protection matters.	TS/SCI
Chief Engineer (if applicable at the Center level)	TS/SCI
Engineering Director	SECRET (TS/SCI preferred)
For Missions Governed by NPR 7120.5, and Crewed Aeronautical Missions	
Program/Project Manager	SECRET (TS/SCI preferred)*
Deputy Program/Project Manager	SECRET
Program/Project Chief Engineer/Lead Mission Systems Engineer, for example: • Program Mission Systems Engineer • Program Chief Engineer • Project Chief Engineer • Project System Engineer • Mission Systems Engineer	SECRET (TS/SCI preferred)*
HSF Vehicle Integration Manager or Vehicle Lead Engineer (other mission types as needed)	TS/SCI
HSF Mission Integration or Operations Manager (other mission types as needed)	TS/SCI
HSF Software and Avionics Manager or Lead Engineer (other mission types as needed)	TS/SCI
System Security Engineer	TS/SCI
Flight subsystem or instrumentation engineers, where the subsystem or instrument is vulnerable to threats, at the discretion of engineering management.	SECRET
Program/Project Safety and Mission Assurance Officer	SECRET
Operations Manager	SECRET

*TS/SCI recommended for Category-1, Risk Class-A missions	
For Missions Governed by 7120.8, and Uncrewed Aeronautical Missions, Balloon Missions	
Program/Project Manager	SECRET
Deputy Program/Project Manager	SECRET
Program/Project Chief Engineer/Mission Systems Engineer	SECRET
Program/Project Safety and Mission Assurance Officer	SECRET

Change Log

Chg#	Approver	Date Approved	Description/Comments
0	PAEP	3/26/2020	The Agency Program Management Council (APMC), in October 2019, issued an action item to SMD and EP to work together to provide informal guidance/best practices for key personnel and roles that should possess security clearances at the appropriate levels for sufficient awareness, mitigation, and implementation of the EP strategy.
1	PAEP	1/4/2021	Added guidance for the clearance levels of Chief Engineers and Engineering Directors per EP Board action 22-1. Added guidance for the clearance levels of System Security Engineers per EP Board #22 discussion.