UK SPACE AGENCY

Unlocking Space
- Clearance and Classification

Introduction

The UK's 2021 National Space Strategy (NSS) identified 10 core goals, of which Goal 4 was to protect and defend our national interests in and through space.

Space is recognised as Critical National Infrastructure (CNI). Taking action to protect and defend in this context would reduce the risk of disruption to the UK economy and/or way of life.

From April-June 2024, the Unlocking Space for Dual Use (USD) team conducted an RFI, yielding 32 responses from industry.

Common themes and challenges were identified, including difficulties related to Clearance and Classification.

While the USD team and wider UKSA cannot grant such clearance, this material should provide insight into the complexities of the subject for academia and industry.

What Is Clearance and Classification?

CLEARANCE:

WHO IS AUTHORISED TO VIEW/HANDLE RESTRICTED INFORMATION.

CLASSIFICATION:

WHAT LEVEL OF RESTRICTION IS APPLIED TO INFORMATION, AS DICTATED BY GOVERNMENT POLICY

Who Does Clearance and Classification Apply To?

Everyone who works with government.

Security clearance underpins work the government do at classified levels and is required for work on government projects that handle sensitive information.

This is associated with any and all security concerns the government may have, as well as national interests.

Government security standards are not the same as private or industry practices.

Trust: the foundation of security clearance

- **Qualified Individuals**: Must be trusted, suitably qualified, and have an acceptable nationality profile (e.g., no dual nationality with restricted countries).
- **HMG Sponsor**: Handles higher classification information via a contractual relationship, often requiring a Security Aspects Letter (e.g., SC or DV clearance).
- **Trade Association Flexibility**: May offer more flexibility in supporting suppliers due to their sector status.
- **Sponsor Role**: A sponsor within the supplier company or outsourced Clearance Administrator manages the individual's application on the National Security Vetting Portal.

Clearance Levels

To give a basic level of assurance related to all staff within government, all government employees regardless of their role will be checked at the **Baseline Personnel Security Standard (BPSS)** level. This covers: Identity (ID); Right to work (RTW) in the UK; Employment history; and Criminal record (unspent convictions). UK residency may affect the checks undertaken.

The next level of clearances are as follows:

Accreditation Check (AC): used particularly for staff in aviation and who have access to secure areas of airports / aircraft.

Counter Terrorism Check (CTC) Level 1B: used particularly for staff who have access to public figures or sites at particular risk of terrorism.

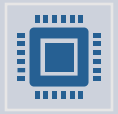
Security Check (SC): most commonly referenced level of clearance for staff who need access to S or occasional access to TS assets

Enhanced Security Check (eSC): where staff need an additional level of assurance but not quite to DV level.

Developed Vetting (DV): where staff need frequent and uncontrolled access to TS assets.

Enhanced DV (eDV): can also be granted and is an even lengthier process than the above, but only a very few individuals need to carry this level of clearance.

Security Controller and Clearance Management



Internal Security Controller Function: Smaller companies may need to establish their own Security Controller function, which requires specialised knowledge and cannot be a side activity due to the high level of assurance and responsibility involved.

Senior Responsibility: This role carries significant responsibility, ideally with a direct line to the CEO/board level, and requires substantial staff time and software to manage clearances and sensitive data, coordinated with HR.

Outsourcing Option: If internal management is not feasible, companies can outsource the initial sponsorship and application process to specialist companies, though the actual vetting process remains within the government.

Ongoing Management: Even with outsourcing, companies must manage personal information of employees undergoing clearance, typically handled by HR in collaboration with the Security Officer.

Individual Responsibilities for Holding Security Clearances

Data Handling: Properly handle data at different classification levels, avoiding printing, transporting, or displaying sensitive information in public or open office environments. Higher classifications may require discussions only in secure, eavesdropping-managed facilities.

Secure Communication: Lock information or notes in a safe and use specific, controlled email systems for sharing sensitive data.

Travel Notifications: Notify the Security Controller for approval before any travel (business or leisure) and agree on IT equipment to be taken overseas, possibly using blank laptops and burner phones in certain countries.

Process within Government

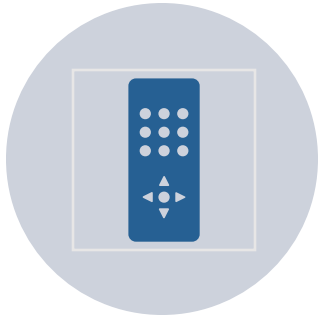
Internal Security Function: Within MoD and across government, an internal security function handles staff applications through the National Security Vetting Portal (NSVP), which is managed by the Cabinet Office.

Role of Security Controller: A Security Controller (or similar role) manages and approves individuals for clearances within government departments. Higher-level clearances involve significant costs due to extensive checks and interviews.

Cost of Clearances: The cost for higher-level clearances like DV can vary widely, involving detailed searches (financial details, record checks) and interviews with staff members and their contacts, making it a time-consuming and expensive process.

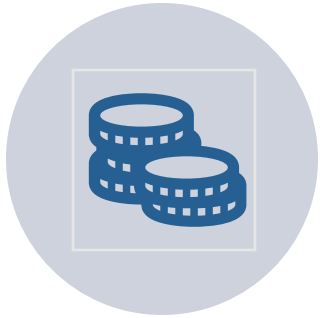
Application Process: Individuals cannot apply for security clearance themselves; it must be requested by the employing company and carried out by government agencies.

Process for Industry



Internal Security Controllers: Larger companies (e.g., Airbus, BAE Systems, Lockheed Martin) with long-standing MOD contracts typically have in-house Security Controllers managing staff clearances and physical security. They may also oversee cyber security in collaboration with the IT/Cyber Security function.

Collaboration with HR: The Security function works closely with HR to manage lower-level checks (e.g., BPSS) and ensure sensitive personal information is handled confidentially.



Investment in Resources: Companies handling clearances in-house may need to invest in specific resources and software to manage the process effectively.

Contractual Initiation: Security clearances for company employees are typically initiated through a contract with HMG, accompanied by a Security Aspects Letter (SAL) detailing the required roles and clearance levels.

Classification

- Levels of classification
- Handling instructions
- Under-classifying and over-classifying information

OFFICIAL

Description: This is the default classification for most government information.

Protection: It includes routine business operations and information that requires protection against accidental or deliberate compromise.

Impact: The compromise of OFFICIAL information could cause limited damage to the UK's interests, such as minor financial loss or inconvenience.

Handling: OFFICIAL information is protected by standard security measures, such as access controls and encryption. It is shared on a need-to-know basis but generally does not require additional protective measures.

OFFICIAL-SENSITIVE

Description: This is a subset of OFFICIAL information that requires additional protection due to its sensitivity.

Impact: The compromise of OFFICIAL-SENSITIVE information could cause more significant damage, such as harm to individuals, damage to the reputation of the organisation, or operational disruption.

Handling: OFFICIAL-SENSITIVE information requires stricter handling measures. This includes enhanced access controls, more rigorous encryption standards, and additional protective markings to ensure that only authorised personnel can access it.

OS is not a substitute for SECRET!

SECRET

- **Description**: This classification is used for more sensitive information that requires a higher level of protection.
- **Protection**: It includes information that could seriously damage the UK's interests if compromised.
- **Impact**: The compromise of SECRET information could lead to serious damage, such as significant financial loss, major operational disruption, or serious harm to individuals.

TOP SECRET

- **Description**: This is the highest classification level and is used for the most sensitive information.
- **Protection**: It includes information that requires the highest level of protection due to its extreme sensitivity.
- **Impact**: The compromise of TOP SECRET information could cause exceptionally grave damage to the UK's interests, such as widespread loss of life, major economic impact, or severe damage to national security.

Handling Instructions

If information is not marked in the correct way, it poses the risk of being shared to and accessed by individuals who shouldn't see it. Handling instructions can be used in conjunction with all classifications, including 'SENSITIVE'.

RECIPIENTS ONLY

- This indicates that the information must be handled on a strict need-to-know basis. This instruction can be used in conjunction with all classifications, including '-SENSITIVE'.

HMG USE ONLY

- This specifically refers to His Majesty's Government and is used to indicate information that is to be shared only with other HMG departments and can be used in conjunction with all the classifications except the 'TOP SECRET' classification.

MOD USE ONLY

- This specifically refers to the Ministry of Defence and indicates that the information is only to be shared within the organisation. However, if necessary, users need to get permission to share with external partners.

Under-classifying Information

- Under-classifying is information being labelled as a lower classification than the level of the details it contains, which are in fact of a higher sensitivity.
- If information is under-classified, it won't be protected to the level that it needs to be. This means that it could be shared and read by individuals who wouldn't have the necessary security clearances should the information have been classified correctly in the first instance.

Over-classifying Information

- Over-classifying is when information that is of lower sensitivity is marked as being higher than it actually is. Under no circumstance should personnel under- or over-classify as a 'just in case' precaution.
- If information is over-classified, there is a high chance that the information will not be seen by the people who need have access to it, should it have been classified appropriately.

Questions?