

KeplerResearch

Security Policy

Standard Practice Procedures (SPP)

Kepler Research Inc
13663 Office Place, Suite 202
Woodbridge VA 22192

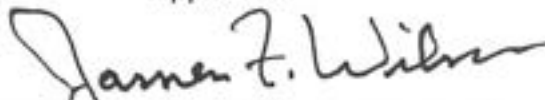
November 2022

Written by



Margie A. Heminger
Facility Security Officer

Approved



James F. Wilson
President & CEO

FOREWORD

Kepler Research Inc., has entered into a security agreement with the Department of Defense (DoD), thereby becoming eligible to perform work on classified contracts. Work of this nature may involve information, material, and knowledge which have a direct bearing on the defense of the nation. Our responsibility as an organization is to safeguard all classified information and material related to these contracts.

This Security Procedures manual has been prepared in an effort to assure that Kepler Research and its employees complies with all applicable requirements of the National Industrial Security Program Operating Manual (NISPOM). The ultimate aim of this document is to prevent disclosure of national security information to unauthorized persons.

The management of Kepler Research supports this facility security program, but security is not just the concern of security personnel; it is an integral part of each employee's job.

Table of Contents

Table of Contents

I. Purpose and Scope.....	5
II. Facility Information	5
A. Facility Clearance	5
B. Storage Capability	5
C. Facility Security Officer	6
D. Key Management Personnel	6
III. Personnel Security Clearances.....	6
A. Purpose and Scope.....	6
B. Clearance Procedures.....	6
C. Access to Classified Documents.....	7
D. Reinvestigations / SF86 Updates.....	7
E. Consultants	7
F. Removal of Access.....	8
IV. Security Education.....	8
A Purpose and Scope.....	8
B. Training/Briefings	8
C. Client Training.....	8
D. Foreign Travel Briefing	8
E. Debriefing.....	9
V. Security Vulnerability Assessments / Self Inspections	9
A. Purpose and Scope.....	9
B. Defense Counterintelligence and Security Agency	9
C. Self-Inspections.....	9
VI. Reporting Responsibilities	9
A. Purpose and Scope.....	9
B. Adverse Information	10
C. Computer / Information System Misuse	11
D. Loss, Compromise, or Suspected Compromise of Classified Information	11
F. Personal Changes	11

VII. Security Violations	13
A. Purpose and Scope.....	13
B. General.....	13
VIII. Department of Defense Hotline	14
IX. Insider Threat Program	15
A. Purpose and Scope.....	15
B. Insider Threat Program Senior Official	15
C. Insider Threat Training.....	15
X. Public Release.....	16
A. Purpose and Scope.....	16
B. Definition	16
C. General.....	16
XI. Classification Review and Release of Information	16
A. Purpose and Scope.....	16
B. General.....	17
C. Totality Aspects of Classification.....	18
XII. Uncleared Locations	18

I. Purpose and Scope

This Standard Practice Procedure (SPP) describes policies regarding the handling and protection of classified information. The SPP is applicable to all cleared employees, subcontractors, consultants, and visitors engaged in cleared contract projects and activities. In the event there is any discrepancy between the SPP and the National Industrial Security Program Operating Manual (NISPOM), the NISPOM shall take precedence.

NOTE: AT THIS TIME KEPLER DOES NOT HAVE CLASSIFIED STORAGE APPROVAL SO NO CLASSIFIED MATERIALS SHOULD BE TAKEN TO A KEPLER OFFICE – ALL CLASSIFIED WORK MUST BE DONE AT A CLIENT SITE.

II. Facility Information

A. Facility Clearance

A Facility Clearance (FCL) is an administrative determination that an entity is eligible for access to classified information or the award of a classified contract. The Defense Counterintelligence and Security Agency (DCSA), which is the Cognizant Security Agency (CSA) for Kepler Research Inc. (Kepler), is the point of contact for any FCL changes.

Kepler currently holds a Top Secret (TS) FCL due to having at least one contract requiring employees access to TS. The FCL is valid for access to classified information at the TS or lower classification level.

At this time, Kepler does not have any subsidiary facilities.

B. Storage Capability

The storage level is separate from the facility clearance level.

At this time, Kepler does not have storage capability for any level of classified documents. Employees will access classified document, if required, only at government facilities.

Teleworking employees will not work on ANY classified documents when at home.

For Kepler to store classified information, it must first have a contractual requirement and receive approval DCSA. If Kepler receives approval for classified storage, the company shall provide suitable protective measures for the safeguarding of classified information, including classified material controlled by the government per government requirements.

Should Kepler obtain classified storage approval, the company will assure that classified information is given or disclosed only to authorized individuals. To this end, employees possessing classified information or material shall determine to what extent other employees, subcontractors, vendors, and suppliers require access to classified information in the performance of tasks or services essential to the fulfillment of the contract or effort.

C. Facility Security Officer

The company shall appoint a U.S. citizen, who is cleared as part of the FCL, as the Facility Security Officer (FSO) to supervise and direct security measures necessary for the proper implementation of the NISPOM and any other furnished guidance or specifications for classification and for safeguarding classified information. Kepler will have at least one alternate FSO. The FSO and other employees who perform duties in direct support of the National Industrial Security Program (NISP) shall complete minimal security training as deemed appropriate by the Cognizant Security Office.

D. Key Management Personnel

Key Management Personnel (KMP) are those individuals who have the authority and responsibility for planning, directing, and controlling cleared facility. The Senior Management Official (SMO), the FSO, and the Insider Threat Senior Official are KMPs who must always be cleared to the level of the company's FCL.

Kepler's Board of Directors will not be required to hold clearances unless they are an active participant in day-to-day operations of Kepler.

III. Personnel Security Clearances

A. Purpose and Scope

To define the requirements of obtaining employee security clearances and processing related clearance downgrading and termination actions.

B. Clearance Procedures

Personnel are processed for a personnel security clearance (PCL) only when it is determined that access to classified information is necessary for performance on a classified contract. The number of employees processed for a clearance will be limited to the minimum necessary for operational efficiency.

Each applicant for a security clearance must produce evidence of U.S. citizenship such as an original birth certificate, passport, or certificate of naturalization. Applicants must also provide the FSO with a digital copy set of fingerprints. The FSO will assist employee to obtain digital fingerprints able to be downloaded to Secure Web Fingerprint Transmission (SWFT).

The FSO will initiate the National Security Positions (SF-86) process in the current DCSA system. Applicants will complete the Questionnaire for SF-86 in the current government system (e-QIP/eAPP). The FSO will ensure the applicant is made aware that the SF-86 is subject to review by the FSO only to determine that the information therein is adequate and complete but will be used for no other purpose at Kepler Research.

While it is Kepler Research that initiates the clearance process for personnel, the U.S. government conducts the investigation and makes the determination of whether an individual is eligible to access classified information and grant the personnel clearance.

The company normally shall not initiate any pre-employment clearance action. However, if deemed necessary by management, the personnel clearance application may be completed by the candidate and submitted by Kepler to the Government prior to the date of employment, provided a written commitment for employment has been made by the company and accepted by the candidate.

C. Access to Classified Documents

Employees will only have access to classified information on a need-to-know basis.

Interim SECRET clearances are not valid for access to Restricted Data; North Atlantic Treaty Organization (NATO); Communications Security (COMSEC); or Sensitive Compartmented Information and Arms Control and Disarmament Agency (ACDA) classified information.

No classified information will be brought into Kepler Research's office space(s); all access to classified information must be done at a government client site or approved subcontractor site.

D. Reinvestigations / SF86 Updates

Cleared individuals are subject to a periodic reinvestigation (PR) or soon to be transitioned to SF86 Updates as part of Government's Continuous Vetting (CV) process every five years, no matter their security clearance lever. The FSO or other security staff is responsible for reviewing PCL records and ensuring personnel are submitted for PRs as required.

E. Consultants

For security administration purposes, consultants are treated as employees and must comply with this SPP and the NISPOM. Consultants with access to classified information will, however, be required to execute a Consultant Agreement which outlines their specific security responsibilities.

F. Removal of Access

The FSO may terminate an individual's PCL when access to classified information is no longer required or as requested per review of security violation or other reason discovered during CV. In general, terminating a PCL when personnel no longer have "need-to-know" will not adversely affect an individual's eligibility to access classified information in the future. At the time a PCL is terminated, the individual will be debriefed by Kepler's FSO and must also debrief from the client's security office.

IV. Security Education

A. Purpose and Scope

To provide briefing and debriefing instructions for cleared employees.

B. Training/Briefings

Security training and briefings shall be provided to employees commensurate with their involvement with classified information.

Kepler Research Training (Initial & Annual):

Prior to being granted access to classified information, employees and consultants must complete client required training and the following Kepler training:

- Kepler's Initial Security Orientation & Awareness Training
- Insider Threat Awareness Briefing
- Counterintelligence Awareness Information
- Cyber Threat Information
- Reporting Requirements
- Whistleblower Briefing
- Controlled Unclassified Information Awareness – for those with a Kepler laptop

Same briefings will be given to employees annually.

C. Client Training

Employees will also be required to complete all required client initial and reoccurring training.

D. Foreign Travel Briefing

Prior to performing any client or personal foreign travel, cleared employees shall be reminded of their individual responsibility not to make unauthorized disclosures of classified information.

Employees will receive a Foreign Travel Briefing and Travel Advisory information taken from the Department of State's website for the specific foreign countries the employee will be traveling to from Kepler's FSO or other security staff personnel.

Kepler's FSO or other security staff personnel will enter the travel and debriefing information in Defense Information System for Security (DISS).

E. Debriefing

Debriefings shall be provided by the FSO or an authorized representative when a cleared individual terminates employment with Kepler or when his/her clearance is terminated for other reasons (access to classified no longer required, or revocation of security clearance by DCSA).

V. Security Vulnerability Assessments / Self Inspections

A. Purpose and Scope

To establish the inspections that Kepler Research is subject to and will conduct.

B. Defense Counterintelligence and Security Agency (DCSA)

The DCSA is the government CSA, which provides oversight of cleared contractors' procedures and practices for safeguarding classified defense information. DCSA Industrial Security Representatives may contact personnel in connection with the conduct of a security vulnerability assessment, as part of an investigation of an unauthorized disclosure of classified information, or to provide advice and assistance on security related issues.

C. Self-Inspections

Security staff will review Kepler's security program on an ongoing basis, but also perform, on an annual basis, and a formal self-inspection using DCSA Self-Inspection Checklist document. The purpose of the self-inspection is to assess security procedures against NISPOM requirements to determine their effectiveness and identify any deficiencies/weaknesses. As part of this self-inspection, cleared personnel interviews can occur. The FSO must certify annually to DCSA that a self-inspection has been completed, the results have been provided to Kepler's President, and a plan has been implemented to address any findings.

VI. Reporting Responsibilities

A. Purpose and Scope

Due to the nature of your position, you have been granted access to classified information that is vital to national security. You are charged with safeguarding that

information. It is both an honor and a privilege that allows you to make a very special contribution to your county. However, it carries certain obligations that you must meet in order to maintain your access.

One of these obligations is to report to your security office/FSO any behaviors, incidents, or events that might in some way impact national security and your ability (or that of your co-worker) to function positively and effectively in a national security environment.

Based on the guidelines set forth in the National Industrial Security Procedures Operating Manual (NISPOM), you should report the following.

When in Doubt – Report!

NOTE: AT THIS TIME KEPLER DOES NOT HAVE CLASSIFIED STORAGE APPROVAL, SO NO CLASSIFIED MATERIALS SHOULD BE TAKEN TO A KEPLER OFFICE – ALL CLASSIFIED WORK MUST BE DONE AT A CLIENT SITE.

B. Adverse Information

Adverse information is any information regarding cleared personnel which suggests that their ability to safeguard classified information may be impaired or that their access to classified information may not be in the interest of national security. **Cleared personnel must report adverse information regarding themselves or another cleared individual** to the FSO, Police, Federal Bureau of Investigation (FBI), and/or DCSA depending on the urgency of an event.

Reportable adverse information includes:

- Threats or knowledge of espionage, sabotage, or subversive activities
- Relationships with any known saboteur, spy, traitor, or anarchist
- Engaging in espionage or acting as an agent of a foreign nation
- Serious mental instability or treatment at any mental institution
- Use of illegal substances or excessive use of alcohol or other prescription drugs
- Excessive debt, including garnishments of wages
- Unexplained affluence/wealth
- Unexplained absence from work for periods of time that is unwarranted or peculiar
- Criminal convictions involving a gross misdemeanor, felony, or court martial
- Violations and deliberate disregard for established security regulations or procedures
- Unauthorized disclosure of classified information
- Members of, or individuals sympathetic to, an organization aiming to overthrow the U.S. Government by unconstitutional means
- Involvement in the theft of, or any damage to, Government property

- Access to classified information that is no longer needed

C. Computer / Information System Misuse

- Unauthorized entry into an automated information system, whether government or contractor, for any reason
- Modification, destruction or manipulation of hardware or software on any government or contractor equipment
- Obtaining/using someone else's password
- Sharing a password
- Using a password to browse through another's account without permission
- Copying/Deleting information on another's account without permission

D. Loss, Compromise, or Suspected Compromise of Classified Information

Cleared personnel must immediately report the loss, compromise, or suspected compromise of classified information.

Report:

- Significant vulnerability in security equipment or hardware/software that could possibly lead to the loss or compromise of classified information
- Inadvertent or deliberate removal of classified information/materials to an unauthorized area
- Inadvertent or deliberate unauthorized destruction of classified information/materials
- Knowledge of a security violation or infraction & not reporting it
- Inoperability of locks, doors, vaults, etc., that are in place to security classified information and/or materials
- Deliberate or inadvertent disclosure of classified information/materials to an unauthorized person
- Loss of classified information/materials
- Request for classified or sensitive information/materials through unauthorized channels

F. Personal Changes

Cleared personnel must report personal changes to the FSO such as:

Changes in Person Status

- Name change
- Marital status change (including legal separation)
- Cohabitation status change (doesn't include non-romantic roommates)

Foreign Travel

- Includes all non-official government business trips and vacations abroad, even day trips to Mexico and Canada.

- If stationed abroad, you must report all personal travel to other countries during that time period.

Foreign Contact

- Someone that could have personal information about you, including details about your life
- Any attempt by a foreign national to solicit sensitive/classified information or other contact that you regard as suspicious
- Close and continuing contact with a foreign national in any capacity in person, by phone, or via internet
- Contact with anyone who works for or is associated with a foreign government or foreign-owned organization or business
- Financial obligations to invest in or employment with foreign nations and/or companies

Financial Problems

- Filing for bankruptcy
- Garnishment of wages
- Having a lien placed on your property for failing to pay a creditor
- Eviction from a residence for failure to pay rent
- Inability to meet all financial commitments

Arrests

- Any arrest - regardless of whether or not charges were filed
- Any general involvement with the legal system (such as being sued, or filing a claim against someone else)

Psychological or Substance Abuse Counseling

Reportable mental health issues include:

- Legal findings of mental incompetence
- Court-ordered mental health care
- In-patient mental health care
- Certain diagnoses which may impair judgement or reliability
- Self-appraised mental health concerns that could impact judgement or reliability

Note: Seeking mental health treatment and counseling in and of itself is NOT a reason to revoke a clearance. Seeking care for personal wellness and recovery may contribute to decisions about your eligibility or continuous evaluation.

VII. Security Violations

A. Purpose and Scope

To establish the method for reporting security violations, and the disciplinary actions to be taken when these violations occur.

NOTE: AT THIS TIME KEPLER DOES NOT HAVE CLASSIFIED STORAGE APPROVAL SO NO CLASSIFIED MATERIALS SHOULD BE TAKEN TO A KEPLER OFFICE – ALL CLASSIFIED WORK MUST BE DONE AT A CLIENT SITE.

B. General

All management and supervisory staff shall ensure that the employees working under their supervision are sufficiently familiar with the Kepler's and their client's security procedures to enable them to comply with those provisions in accomplishing their assigned duties. Remember – at this time, Kepler does not allow ANY classified documents in Kepler office space – all must be kept at a client site.

The FSO shall provide advice and assistance on all security matters upon request of management, supervisors, or employees.

Should Kepler's office space ever have classified storage, the FSO shall conduct routine inspections throughout the space to ensure that necessary security precautions are being taken to protect classified information at all times.

If an employee discovers a security violation, they must report it immediately to the FSO.

C. Procedure – if Kepler has classified storage/if violation happened at a client site the client's Security Officer must be immediately notified.

Requirements for Reporting Security Violations - When a security violation occurs, thereby permitting a possible or actual compromise of classified information as determined by the FSO, the following procedures will apply:

1. The FSO, the manager or supervisor involved, and Kepler's Information Technology (IT) Security Point of Contact (POC) shall investigate the security violation to determine the severity and extent of the possible compromise of classified information.
2. The investigation will include, but will not be limited to:
 - Determination if material has been lost or if compromise is suspected
 - The violation or practice which led to the loss or compromise

- Proposed corrective action to ensure that a similar incident shall not recur

The government organization owning the classified document will be notified.

3. The FSO shall prepare a report on the violation within 48 hours after receiving notification of the violation. This report shall be submitted to the responsible manager or supervisor, the government client, and a copy forwarded to the local DCSA Office if the seriousness of the violation so warrants (i.e., if a loss, compromise, or suspected compromise of classified occurred).

The FSO's report will include:

- Identity of the classified information or material involved
- A resume of the essential facts surrounding the incident
- The name, social security number, date and place of birth, and position of the individual(s) primarily responsible for the incident, including a record of prior loss, compromise or suspected compromise, if any
- A statement of the corrective action taken to prevent a recurrence of similar incidents
- Specific reasons for concluding: (1) loss or compromise occurred; (2) compromise is or is not suspected; or (3) compromise did not occur
- If compromise or suspected compromise of classified information occurred while such information was in the U.S. postal system, the FSO shall promptly notify the appropriate Postal Inspector

4. Disciplinary action taken by Kepler Research is based upon a review of each case's own merits. The seriousness of the violation will be determined by whether a compromise, suspected compromise, or loss of classified information has occurred, or if it was only administrative in nature. Disciplinary action may be any one or more of the following depending upon the above factors: counseling and verbal warning, additional training, a written reprimand, revocation of security clearance, dismissal from the University or its subsidiary, or even criminal filing.

VIII. Department of Defense (DoD) Hotline

The DoD provides a Defense Hotline as a confidential avenue for individuals to report allegations of wrongdoing pertaining to programs, personnel, and operations that fall under the purview of the DoD, pursuant to the Inspector

General Act of 1978. Anyone, including members of the public, DoD personnel and DoD contractor employees, may file a complaint with the DoD Hotline.

Hotline Phone Number: 800-424-9098 / 703-604-8799

Hotline Fax: 703-604-8567

To report online: <https://www.dodig.mil/components/administrative-investigations/DoD-hotline/>

IX. Insider Threat Program

A. Purpose and Scope

Kepler Research has developed a written corporate-wide Insider Threat Program Plan, signed by the President, describing:

- Capability to gather relevant insider threat information across functional areas (e.g., human resources, security, information assurance, legal)
- Procedures to (1) access, share, compile, identify, collaborate among functional elements, and report relevant information that may be indicative of a potential or actual insider threat; (2) deter cleared personnel from becoming insider threats; (3) detect insiders who pose a risk to classified information; and (4) to mitigate the risk of an insider threat

B. Insider Threat Program Senior Official

The Insider Threat Program Senior Official (ITPSO) will be Kepler's FSO or Kepler's President. The ITPSO is a KMP who is cleared in connection with the FCL and is responsible for establishing and executing company-wide Insider Threat Program. Other personnel may form a working group to assist the ITPSO with their duties.

C. Insider Threat Training

Within thirty (30) days of being assigned duties related to Insider Threat Program Management, the ITPSO and working group personnel must complete training that addresses:

- Counterintelligence and security fundamentals, including applicable legal issues
- Procedures for conducting insider threat response actions
- Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information
- Applicable legal, civil liberties, and privacy policies

All cleared personnel must complete their insider threat awareness training before being granted access to classified information and annually thereafter. Training will include, at a minimum:

- The importance of detecting potential insider threats by cleared employees and reporting suspected activity to the insider threat program designee
- Methodologies of adversaries to recruit insiders and collect classified information
- Indicators of insider threat behavior and procedures to report such behavior
- Counterintelligence and security reporting requirements, as applicable

X. Public Release

A. Purpose and Scope

To provide instructions pertaining to the public release of information on classified projects or contracts.

B. Definition

Public Disclosure - The passing of information and/or materials pertaining to a classified contract to the public or any member of the public by any means of communications.

C. General

- Prior approval of the User Agency's Contracting Officer is required for any public release of information (classified or unclassified)
- Contact Kepler's FSO or Contracting Officer to view the DD 254, providing specific requirements for public releases.

XI. Classification Review and Release of Information

A. Purpose and Scope

To establish the requirements of a Security Classification Management Program designed to ensure the proper identification, classification, and marking of information concerned with the National Defense in accordance with government guidance documents, e.g., "Contract Security Classification Specifications" (DD Form 254).

NOTE: AT THIS TIME KEPLER DOES NOT HAVE CLASSIFIED STORAGE APPROVAL SO NO CLASSIFIED MATERIALS SHOULD BE TAKEN TO A KEPLER OFFICE – ALL CLASSIFIED WORK MUST BE DONE AT A CLIENT SITE.

B. General

The FSO is responsible for all external contact and correspondence that relates to matters of security classification requirements and is the central control point for coordinating all matters that relate to the assignment of security classifications.

Individuals receiving classification guidance from external sources, written or verbal, shall transmit such information to the FSO for the updating of central classification records and the proper notification to other concerned parties.

Employees who are responsible for generating classified material or have the technical supervisory responsibility of reviewing material for proper classification are encouraged to contribute to the program by making recommendations for regarding action whenever possible, and to bring to the attention of the FSO inconsistencies in security classification guidance.

The FSO, when requested, shall assist in proposal preparation by providing clarification and elaboration of security classification guidance furnished with the Request for Proposal (RFP). This will include assisting in the development of a detailed security classification guidance document, where appropriate.

It is the responsibility of each employee preparing material to classify it at as low a level as possible, consistent with current security classification guidance. Any classified information not specifically required for presentation shall be omitted from proposals and reports. Employees must always follow client requirements and have their work reviewed by the client as required.

Managers and supervisors shall maintain close supervision of personnel responsible for classifying information and shall assist in the review and assignment of correct security classifications based on their security clearance and "need-to-know."

Determination of Classification – Coordinate with your government client.

Unsolicited Proposal or Non-Contractual Material - In developing a classification for an unsolicited proposal or originating information not in the performance of a contract, the following rules shall apply:

- If information is included in the proposal or other material which can be identified as being classified, the proposal or other material shall be marked with the appropriate classification.
- If information is included in the proposal or other material which cannot be identified as being classified or for which there is no security guidance, and it is believed that the proposal or other material contains information which should be classified, it shall be marked with a preliminary classification at the

appropriate level utilizing the following notation only on the cover or first page:
"Classification Determination Pending. Protect as though Classified Secret."

- If a preliminary classification is not assigned or if security guidance is inadequate and a decision cannot be reached, contact the FSO for assistance in obtaining classification interpretation and/or determination by the appropriate Government agency.
- If a preliminary classification is assigned, the following shall apply:
 - Access to the information will be limited to the minimum number of employees practicable.
 - The individuals selected to have access to the information will be limited to cleared U.S. citizens who will be advised of the importance of the information.
 - When not in use, documents containing the information should be stored in an approved security container.
 - Secure methods of transmittal are to be used for transmitting the material between personnel or locations.
 - Reproduction of the information should be kept at a minimum.

C. Totality Aspects of Classification

The overall classification of a document will normally be equal to the highest classification assigned to any of its pages.

It is possible that two or more items of information, each properly classified at a lower level, will, when contained in the same document, require a higher classification level. When such a situation exists, the document shall carry the higher classification and the following statement shall appear once on the inside of the front cover, and on the title page, or on the first page of the document.

"Although the classification of the information on each page of this document is no higher than indicated by the markings thereon, the association of information requires protection at the higher level applied as the overall classification."

XII. Uncleared Locations

(At this time, Kepler only has one office)

NOTE: AT THIS TIME, KEPLER DOES NOT HAVE CLASSIFIED STORAGE APPROVAL SO NO CLASSIFIED MATERIALS SHOULD BE TAKEN TO A KEPLER OFFICE – ALL CLASSIFIED WORK MUST BE DONE AT A CLIENT SITE.

Cleared employees physically located at an uncleared location will be briefed by the FSO of the home office or a principal management facility, or by a designated representative at the uncleared location.

Recurring briefings will be conducted during visits by the FSO to the location, during a visit by the employee to the cleared facility, or by the use of audiovisual or written materials.

Written confirmation will be maintained by the home office or a principal management facility of all briefings to cleared employees.