**Questions when Interviewing Uncleared Employees**

* Facility
  + Who is your Facility Security Officer (FSO), Alternate Facility Security Officer and Information Systems Security Manager (ISSM)?
    - John Smith is the FSO
    - Jane Doe is the AFSO
    - Jan Smith is the ISSM
* CUI
  + What is Controlled Unclassified Information (CUI)?
    - Controlled Unclassified Information (CUI) is unclassified information requiring safeguarding and dissemination controls, consistent with applicable law, regulation, or government-wide policy.
  + Why is CUI important?
    - Information designated as CUI has the same intrinsic value and potential adverse impact if compromised
  + How does CUI relate to your position?
    - Explain how you have access to CUI in your everyday work environment.
* Classified Information
  + What is classified information?
    - Classified information is categorized into three classification levels, Confidential,

Secret, and Top Secret. Classification levels are applied to national security information that, if subject to unauthorized disclosure, could reasonably be expected to cause damage, serious damage, or exceptionally grave damage to national security. Each classification level has its own requirements for safeguarding. The higher the level of classification, the more protection the classified information requires to reasonably prevent the possibility of its loss or compromise.

* + How would you know if something was classified?
    - Classified information will be marked with the words CONFIDENTIAL, SECRET or TOP SECRET
  + If you found unprotected classified information what would you do?
    - Secure the classified material and contact security
  + Have you ever heard classified information being discussed?
    - The employee can answer yes or no and caveat a yes with I always contact security prior to having a classified conversation or meeting for proper guidance.
  + Have you ever come into possession of classified materials? How?
    - Employee can explain as applicable

**Questions when Interviewing Cleared Employees**

* Cleared Roles and Responsibilities
  + What is your job title/responsibility?
    - Employee can explain as applicable
  + What is the level of your security clearance? How long have you been cleared?
    - Employee can explain as applicable
  + Why are you cleared (describe the contract or programs that require you to be cleared)?
    - Employee can explain as applicable
  + If recently cleared, what were the processes/steps in applying for your security clearance?
    - Explain that the program manager made a decision that access to classified material was necessary in the performance of my duties, a request for clearance was put in through the PERSEC office and a clearance investigation was initiated.
* Training and General Knowledge
  + When was your last security briefing? What do you recall from that briefing?
    - June of 2022
  + Can you recall any of the following topics being addressed in briefings? Risk Management, Job Specific Security Brief, Public Release, Safeguarding Responsibilities, Adverse Information, Cybersecurity, Counterintelligence Awareness, Insider Threat
    - All were part of the 2021 Annual Security Refresher Training
* Access to Classified Information
  + When was your last access to classified information and at what level?
    - Explain any access to classified information
  + Have you ever accessed classified information outside of this facility?
    - This answer should always be no
  + Do you have the combination to any storage containers, access to any closed areas, etc.?
    - Yes or no answer
  + What are the security requirements regarding combinations to security containers?
    - Combinations of GSA approved storage containers are classified at the same level as the highest level of material stored in the container.
    - Commit combinations to memory—DO NOT WRITE THEM DOWN!
    - Protect classified combinations in the same manner as any classified document.
  + Who, other than yourself, has access to these containers?
    - Only properly cleared individuals with need-to-know
  + How do you keep track or maintain your knowledge of the combination?
    - Combinations are committed to memory
  + Is a record maintained of the safe combination? If so, where?
    - Yes, created and maintained by security, classified combinations are treated like any other classified document.
* Protection
  + Where do you typically work on classified information?
    - Open Storage or Restricted Area designated for classified processing.
  + What procedures do you follow to protect classified information while working on it?
    - I follow the Standard Security Operating Instructions (SSOI’s) found on the Brevard County Security Sharecenter.
* CUI
  + What is Controlled Unclassified Information (CUI)?
    - Controlled Unclassified Information (CUI) is unclassified information requiring safeguarding and dissemination controls, consistent with applicable law, regulation, or government-wide policy.
  + Why is CUI important?
    - Information designated as CUI has the same intrinsic value and potential adverse impact if compromised
  + How does CUI relate to your position?
    - Explain how you have access to CUI in your everyday work environment.
* Visit Support
  + What are the procedures for visitors coming here for a classified visit?
    - Refer to
      * SSOI-02 Classified Visits and Meetings
      * SSOI-07 International Visits
      * SSOI-31 Brevard County Visitor Control Procedure
      * SSOI-32 Brevard County Host and Escort Procedures.
  + What are the procedures for individuals going on classified visits?
    - Submit a Visit Authorization Request (VAR) through DISS to the host facilities SMO.
  + What are the procedures to debrief individuals returning from classified visits?
    - * SSOI-02 Classified Visits and Meetings
      * SSOI-07 International Visits
  + What are the procedures for securing classified information brought back to the facility?
    - All classified material brought back from a classified meeting will be brought into accountability, and stored in a classified container.
  + What are the procedures for determining need-to-know and giving visitors access to classified information?
    - SSOI-02 Classified Visits and Meetings
* Contacts
  + Have you ever been approached by anyone requesting classified information?
    - Yes or no
  + Do you ever work overtime and access classified information?
    - Yes or no
  + What is meant by the term adverse information and how would you report it?
    - Adverse information consists of any information that negatively reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security
  + Can you recall any other reportable items?
    - Yes or no
  + What is an insider threat?
    - L3Harris employees or visitors who will use his or her authorized access, wittingly or unwittingly, to do harm to the security of the United States.
  + What are some indicators of insider threat behavior and who would you report this to?
    - Significant changes in personality, behavior, or work habits
    - Substance abuse or addictive behaviors (e.g., alcohol and drug abuse/gambling)
    - Considerable financial change (e.g., unexplained affluence or excessive debt)
    - Disgruntled to the point of wanting to retaliate
    - Disregard for security procedures and protocols
    - Seeking access to classified or proprietary information and systems/technology without a “need-to-know”
    - Access to facilities and/or proprietary information outside of normal work hours
    - Unauthorized removal, or unnecessary copying or hoarding of classified or proprietary material
  + Can you recall any methods used to recruit trusted insiders?
    - The promise of financial gain
    - Blackmail
    - Gaining trust through personal relationships
    - Seeking out disgruntled employees
* Reporting
  + What is meant by the term "suspicious contact" and how would you report one?
    - Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee, as well as all contacts with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country.
    - Report all suspicious contacts to the FSO or your program security representative
  + Have you ever been cited for a security violation, infraction, or incident?
    - Yes or No
  + What would you do if you committed a security violation, infraction, or discovered one?
    - Report it immediately to the FSO or my program security representative
* Classification Responsibilities
  + Do you generate or derivatively classify information? Tell me about it.
    - Yes or no
  + What security controls are established?
    - Prior to becoming a Derivative Classifier, properly cleared individuals are identified by their program managers and are required to take Derivative Classifier Training initially, then once every two years afterwards.
    - All derivative classified documents and media must be properly marked, protected and stored at the appropriate classification level.
  + How do you know it's classified?
    - All classified information requires classification markings, at the top and bottom of each page, and classified portion markings.
  + Describe the training you received prior to derivatively classifying or generating classified information.
    - Derivative Classifier Training
  + What do you do with classified information?
    - Explain how you use the classified information
  + Do you ever use a computer to generate classified information?
    - Yes or No
  + How do you mark this information?
    - IAW the source document, SCG or current classified marking guide.
  + What information or references do you use when classifying information?
    - The source document or SCG
  + Please produce the classification guidance that you used. Is it accurate?
    - All programs have a Security Classification Guide (SCG), all are up to date
  + What would you do if you determined that the classification guidance was not accurate?
    - I would bring it to the attention of my FSO and my FSO would challenge the classification to the government customer, if warranted.
  + What are the security procedures for publishing classified material?
    - Contractors are not authorized to disclose classified information to the public.