INSIDER THREAT JOB AID

Employment Application Risks and Mitigation for Insiders with National Security Eligibility

Center for Development of Security Excellence
CDSE

The purpose of this job aid is to help insiders with National Security Eligibility understand the risks associated with job searching; to provide guidance on how to be vigilant of threats and evade targeting by malicious actors, while seeking employment. The information in this job aid includes, but is not limited to: mindfulness of posting sensitive information on resumes, vetting and conducting research on recruiters and potential employers, understanding your Non-Disclosure Agreement, requesting a pre-publication or security review and resources for further exploitation and awareness.

CONTENTS

Click the individual links to view each topic.

Introduction 4

Resume Advisory 4

Professional Resume Writing and Career Coaching Services 5

Employment Services Websites and Online Job Boards 5

Social Media-Based Professional Networking 5

Vetting Recruiters 6

Networking and Job Hunting at Events 7

Senior Executive Advisory 7

Beware of Job Scams 8

Exit Interviewing of Departing Employees 9

Resources for Further Exploitation 10

Introduction

A well organized and current resume is often the first step in applying for a job. The application process could include completing questionnaires, providing biographic and contact information, references, documents, academic transcripts, writing samples, certifications, and even performance evaluations. During the application process, you may be contacted by a recruiter. They will most likely want to conduct an initial candidate screening and possibly schedule an interview. An interview may be conducted in-person, by telephone, virtually, or a combination of the three.

Employees who are granted National Security Eligibility (NSE) may include U.S. military personnel, DOD civilian employees, Federal employees, contractors, Federally Funded Research and Development Centers, Think Tanks and Defense Industrial Base employees, among others.

NSE employees must be careful that information provided during a job application does not lead to unauthorized disclosure of classified or Controlled Unclassified Information (CUI) or make them an easier target of malicious actors.

Resume Advisory

It is understandable to provide pertinent details regarding your work experience in the form of duties, skills, and accomplishments. However, you should be careful about specificity and the amount of details in a resume as they can draw the attention of malicious actors. Threat actors can put together, or "aggregate," small details to deduce enough information about U.S. Government activities, military plans, and operations. Resumes can be a "goldmine" of information for adversaries. Malicious actors such as foreign intelligence services or cyber actors can glean valuable information from resumes to target NSE employees. Such targeting can include social engineering, elicitation, unsolicited emails, recruitments, and intrusion and collection from Personal Electronic Devices (PEDs). An NSE employee should have a draft resume reviewed by an agency's or employer's security staff or Facility Security Officers (FSOs).

DO'S

- Security Clearance and Polygraph Information
- Describe projects in an Unclassified manner highlighting your skills and work
- Specific skills certifications e.g. CPA
- Foreign language proficiencies and utilization; e.g. liguist, translator
- General Information Technology skills to include industry-recognized software and hardware systems

DONT'S

- Sensitive Mission descriptions; Project Names
- Specific locations of a classified activity
- Specific dates and locations of operations
- Classified training e.g. specific intelligence tradecraft training
- Budget, personnel strength and information systems of sensitive programs
- Operational jargon
- Classified agency databases

Professional Resume Writing and Career Coaching Services

Be mindful when using professional resume writers or online resume and career coaching services. Most of these services have an online presence and would require you to upload work history and biographic data, in addition to completing detailed questionnaires. But before you avail such services, do your due diligence. Check to see if these services originate from overseas. Research their business practices, reputation, privacy rules, and terms of service. A resume coach may schedule a meeting with you in-person or in a virtual setting. Be mindful of how much detail you provide during such a meeting and be careful not to divulge any sensitive information.

Employment Services Websites and Online Job Boards

Before you upload or post your resume on an online job board or employment website, consider these issues: Some employment or career services websites are headquartered or incorporated in foreign countries or have foreign affiliates or subsidiaries. Anytime you access the website or its mobile application, you may be agreeing to terms and conditions that open you up to their foreign business entities. An employment website may not exercise any control nor be held responsible for third parties who post job advertisements or other content on it. These websites may not be able to authenticate their users. They may also provide user information to foreign law enforcement, security, and intelligence services.

These websites may store and process user data in foreign countries, which may not have the same data protection laws as the United States. Also, users such as recruiters, HR professionals and employers who pay a subscription can download resumes and other applicant information in large batches on a periodic basis from anywhere in the world. These parties may not be held to the same privacy rules and accountability standards as in the United States. It is advisable to read the terms of service and privacy policies of an employment website before registering as a user and uploading a resume, biographic data, and other information.

It is prudent to apply through an online job application form directly on an employer's website rather than posting resumes on an employment website. Employment websites that have multi-factor authentication security features such as USAJOBS.gov, clearancejobs.com, or any employer websites that are password-protected are safer that websites where the connection is unsecure or unencrypted.

Social Media-Based Professional Networking

"Intelligence agencies have always used open source intelligence to spot people with access to the programs or information they are attempting to collect.

The internet provides such agencies with more open source information than ever; some sites, such as LinkedIn, are particularly useful for spotting people with access to desired information or technologies."

- Article "Espionage and LinkedIn: How Not to Be Recruited As a Spy", RANE, July 2, 2019

In September 2020, The FBI and the National Counterintelligence and Security Center (NCSC) released a new movie, "The Nevernight Connection." The movie was inspired by the case of former CIA officer Kevin Mallory and details the fictional account of a former U.S. Intelligence Community official who was targeted by China via a fake profile on a professional networking site and recruited to turn over classified information before being arrested. The purpose of the movie is to increase awareness of how foreign intelligence entities use fake profiles (or personas) and other forms of deception on social media platforms to target individuals in government, business, and academic communities for recruitment and information collection. In April 2021, The United Kingdom's Security Service, MI5, publicly stated that, over a five-year period, at least 10,000 UK nationals were approached by fake profiles linked to hostile states on a popular social media-networking website. These fake profiles targeted virtually every government department and key industries in the UK. And in December 2017, Germany's domestic intelligence agency, BfV, publicly acknowledged that China used fake profiles on the networking website, LinkedIn, to collect information on 10,000 German nationals including politicians.

You must be on-guard that fake profiles (personas) will target you as an NSE employee. Evaluate profiles that want to connect with you. Suspicious or fake profile indicators may include the use of generic names, and fake or absent profile images. Other indicators include a mismatch between current position and work history, many grammatical and spelling errors in profile description, and absence of any voluntary after-work activities, memberships, or associations. Diligence is important as fake profiles will connect with you to gain credibility and then target others connected to you.

Report any suspicious social network contacts to your employer's security office. Reporting is not only required under the National Security Adjudicative Guidelines, but supports the counterintelligence mission of the U.S. Intelligence Community to detect, deter, and counter malicious actors.

Vetting Recruiters

Now that you have been contacted by a recruiter, headhunter, or staffing specialist after posting your resume, what do you do? Do not commit immediately to an interview unless you are confident and knowledgeable about the employer or received a personal referral. It is prudent not to trust an initial contact from an unknown recruiter until you have had an opportunity to independently verify.

Here are some data checks you can do to verify a recruiter:

- Utilize business information services such as Dunn and Bradstreet, Bloomberg, and Better Business Bureau to conduct employer vetting.

- If a recruiter provides contact information that consists of a free web-based email service such as gmail.com, then it could be a potential risk. Same would be for a phone number with an international dialing code or a suspicious caller ID. If needed, call the employer's phone number on its website and verify the recruiter's identity.

Potential Risk Indicators of a Suspicious Recruiter or Interviewer:

- Barely any useful information on recruiter or employer's website and no posted job vacancies
- Unencrypted HTTP website
- No interview time limit, "I have all day"
- Heavy-accented English speaker
- Excessive interest and questioning on specific assignments, dates, mission details, locations or specifics of technology work
- Suspicious U.S. Government affiliation – "I am from the CIA" (Unless you applied through a U.S. Government or agency specific candidate application portal such as USAJOBS.gov)
- Offer of "Consulting gig" rather than employment
- A job offer that has no requirement for a background check
- Excessively high salary or piece work compensation offer
- During a virtual interview, a third person is connected to the meeting but does not communicate
- Scheduling a second interview in-person at a restaurant or hotel room and not in a corporate office
- Paying for a meal and/or offering a gift
- Changing method of communication for future contact
- Introducing a senior colleague or fellow recruiter without informing you; the second individual asks more intrusive questions
- Using ethnicity to stir up emotions in an effort to recruit, appealing to the proverbial "Bamboo Ceiling"

Networking and Job Hunting at Events

NSE employees should be careful and diligent about contacts during networking opportunities at events that are open to the public such as conferences, expositions, symposiums, seminars, industry meetings and other meet-ups. It is a requirement to report any foreign or suspicious contacts during such events, whether you are looking for a job or it's a regular part of your official duties. Such networking events are prime targets for foreign intelligence officers (FIOs) to spot and assess individuals who have access to sensitive information. If you are looking for a job or earning opportunity, you can be susceptible to FIOs who can pose as recruiters or consultants. It is prudent not to commit immediately to an offer of employment, rather take some time to conduct due diligence on a recruiter and a potential employer before further contacts.

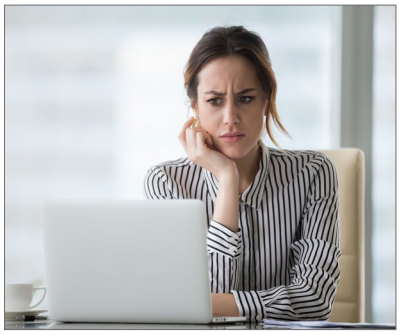
Senior Executive Advisory

NSE employees may consist of former or retired senior grade employees, Senior Executive Service members, retired or transitioning U.S. military field grade officers, and private sector senior executives. They should be mindful of the details in their resumes, including information supporting Executive Core Qualifications that may inadvertently divulge classified information or draw attention from malicious actors. They should also be careful not to divulge any sensitive information when utilizing resume preparation and executive coaching services.

Senior execs should be particularly careful of their presence on professional networking websites. There are online networking services that cater specifically to senior execs that provide networking services for a membership fee or subscription. These websites may not take any responsibility or bear liability for third party content and links to external websites. Senior execs should also remain vigilant and carefully evaluate contact requests from various profiles (personas). Adversaries and malicious actors may use fake profiles to connect with senior executives who not only have access to sensitive information, but also have access to other executives or organization insiders. A fake profile gains credibility once it connects to a senior exec and then moves to connect with insiders. Malicious actors lurking behind these fake profiles may then utilize social engineering to deceive and collect sensitive information. Lastly, senior execs should be careful when connecting to profiles of executives outside their organizations. They should ensure that connections are made with authentic profiles. There are plenty of profiles with the same names. For example, the CEO of a large, publicly-traded company may not have a presence in any networking websites, but there may be thousands of profiles with the same name.

Many global headhunting, executive search, and consulting firms specialize in talent spotting and recruitment of senior execs for employers in Government, academic institutions, and industry. These firms often require candidates to provide detailed resumes and answer specialized questionnaires. Candidates may also be required to meet in-person for interviews in confidential settings. These activities enable executive recruiting consultants to match a candidate against a carefully crafted candidate profile. The consultant then forwards a potential candidate or candidate pool to an employer for an interview. It is therefore important that an NSE senior exec does due diligence when in contact with an executive search firm and report any suspicious contacts or self-report any unauthorized disclosure of classified or CUI information.

Beware of Job Scams



The U.S. Federal Trade Commission (FTC) links job scams to scammers who advertise jobs in the same way legitimate employers do - online (in advertisements, on job sites, and social media), in newspapers, and sometimes on TV and radio. They promise you a job, but what they want is your money and your personal information.

Examples of job scams are:

- Work-from-home job scams
- Nanny, caregiver, and virtual personal assistant job scams
- Mystery shopper scams
- Job placement service scams
- Government and postal job scams

If you see or lose money to a job scam, report it to the FTC at **ReportFraud.ftc.gov**. You can also report it to your state attorney general. For more information, refer to **https://consumer.ftc.gov/articles/job-scams**.

Exit Interviewing of Departing Employees

HR plays a critical role before an employee departs. An Insider Threat briefing must be integrated in an out-processing checklist along with a security debriefing. The employee must be provided points of contact for adverse reporting including security managers, FSOs or their designees, and the FBI. It is important that a departing employee clearly understands that signing a Non-Disclosure Agreement (NDA) such as a SF form 312 is a promise and a responsibility to protect classified information for life, the failure of which would result in penalties under federal law.

Security Debriefing Acknowledgement

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or trasmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

Lastly, an employee should understand that pre-publication materials such as books, manuscripts, speeches, and articles must be submitted to an agency or department's prepublication review office such as the Defense Office of Prepublication and Security Review (DOPSR).

Remain vigilant of risks associated with online job applications and professional networking sites. Be careful to avoid becoming an unwitting insider threat, as you seek employment opportunities inside and outside the national security community.

Resources for Further Exploitation

NSA: Resume Do's and Don'ts
(https://www.nsa.gov/Portals/75/documents/resources/everyone/prepub/resume-dos-donts.pdf)

CDSE Social Media Smart Card
(https://www.cdse.edu/Portals/124/Documents/jobaids/cyber/LinkedIn_Smartcard_Trifold.pdf)

FBI: The Nevernight Connection
(https://www.fbi.gov/video-repository/nevernight-connection-093020.mp4/view)

How to Highlight Your Security-Cleared Skills on Your Resume, Without Revealing Classified Information
(https://news.clearancejobs.com/2012/06/11/how-to-highlight-your-security-cleared-skills-on-your-resume-without-revealing-classified-information/)

Federal Trade Commission Consumer Advice: Job Scams
(https://consumer.ftc.gov/articles/job-scams)

CDSE Derivative Classification Job Aid
(https://www.cdse.edu/Portals/124/Documents/jobaids/information/DerivativeClassification.pdf)

Defense Office of Prepublication and Security Review (DOPSR)
(https://www.esd.whs.mil/Security-Review/PrePublication-and-Manuscripts/)

CDSE Termination Briefing Short
(https://securityawareness.dcsa.mil/cdse/multimedia/shorts/termination/story_html5.html)