



INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE



JUNE 2022

Promoting Cultural Diversity in the Intelligence Community:

Recruiting and Clearing Personnel with Foreign Ties

Presented by

INSA'S SECURITY POLICY REFORM COUNCIL

Building a Stronger Intelligence Community

A diverse workforce strengthens and enriches the Intelligence Community (IC) in many ways. Hiring individuals with different backgrounds and experiences fosters new ideas, challenges traditional biases, and draws on extensive cultural knowledge present in the American population. However, while the benefits of culturally diverse employees are well-understood in the IC, the security clearance process does not lend itself to hiring and clearing such individuals in a timely or effective manner. From a security perspective, the vital component for success in hiring individuals with foreign affiliations is establishing a responsive, adaptive, and effective background investigations program that is inclusive of the global environment.

The Director of National Intelligence (DNI) has established a goal to increase diversity in the national security workforce, which encompasses federal employees and industry, as part of a comprehensive diversity strategy.¹ While the notion of a diverse population covers a broad spectrum of demographics, one vital part is the recruitment, retention, and promotion of personnel with critical skill sets who are increasingly global in their backgrounds, life experiences, and associations. Such candidates possess first-hand international education, global life experiences, cultural awareness, native language speaking abilities, regional expertise, and keen analytical perspectives—all traits ODNI characterizes as enhancing IC mission performance.

To explore the challenges to onboarding individuals with such vital skills and perspectives, this paper focuses on the recruitment and retention of personnel who possess foreign ties, as well as the identification of solutions to enhance the vetting and adjudication of security clearances for these individuals.

BACKGROUND

One in eight residents of the United States is a native-born U.S. citizen with at least one immigrant parent.² These Americans—roughly 41 million people—have unique language skills and insights into their families’ homelands that would be of great value to the IC. At the same time, from a security perspective, these overseas family ties create potential risks that must be identified and mitigated during the security clearance process.

In a marketplace characterized by a global competition for talent, the most qualified individuals for critical positions frequently have personal histories that tie them to foreign countries, either through travel, overseas living, or personal, professional, or familial ties to non-U.S. nationals. In addition to cultural and language skills, the IC also needs employees with Science, Technology, Engineering, and Math (STEM) skills that are in high demand in the commercial sector. Nearly half of the full-time graduate students in U.S. natural sciences and engineering programs are foreign-born, according to the National Science Foundation.³ U.S. citizens in this group—some of whom have a desire to pursue careers in public service⁴—represent highly skilled candidates for cleared employment, yet have difficulty making it through the security process due to their foreign ties.

Some of the information that background investigations are designed to gather can be difficult to compile when a candidate has spent significant time traveling or living overseas or if a candidate has large numbers of foreign contacts

or family members—principally because it can be difficult to access reliable information in many foreign countries. Investigators typically interview candidates’ neighbors for insights into their behavior, for example, which may not be possible overseas. And it can be difficult to assess whether a candidate’s ties to foreign nationals pose security risks if those foreigners’ own backgrounds cannot be evaluated. Candidates with foreign connections who cannot be vetted are often denied a clearance, as the investigative process is designed to eliminate any potential risk rather than to manage and mitigate it.

To attract top talent possessing technical skills and global perspectives, the IC’s security apparatus must re-examine historical assumptions about the risks posed to national security by foreign-born persons or those with close foreign ties. The answer is not to lower security standards, but rather to perceive risk as something to be mitigated

rather than eliminated, and to apply newly introduced (and universal) screening and monitoring procedures to assess the risks, if any, of employees’ foreign connections.



To attract top talent possessing technical skills and global perspectives, the Intelligence Community's security apparatus must re-examine historical assumptions about the risks posed to national security by foreign-born persons or those with close foreign ties.

OLD AND NEW WAYS FOR ASSESSING FOREIGN TIES

Longstanding approaches prioritizing risk avoidance must be overcome by a new risk-mitigation paradigm. Foreign affiliation or affinity is but one factor in determining suitability, fitness, and eligibility for the award of a security clearance—one that is balanced against the imperative to hire staff with the skills to address pressing national security challenges. In fact, the national security adjudicative guidelines explicitly state that any doubt shall always be decided in favor of national security, which for some “checklist oriented” personnel may promote a risk-averse paradigm.

The government’s security apparatus has traditionally viewed foreign backgrounds and affiliations as creating risk. The National Security Adjudicative Guidelines⁵ used for granting and revoking security clearances consider three types of potentially malign foreign ties in a candidate’s background: Allegiance to the United States (Guideline A); Foreign Influence (Guideline B); and Foreign Preference (Guideline C). Candidates with such ties have found that federal agencies primarily focus on the *security concerns* centering around an individual’s potential risks and vulnerabilities, rather than considering relevant *mitigating factors and measures*. Risk mitigation factors could include the limited frequency with which a candidate travels overseas or contacts foreign family members; the absence of known government connections of overseas family members; and the extent to which the government of the candidate’s country of heritage is known to exploit diaspora members’ access. Risk mitigation measures that may be instituted after a candidate’s clearance could include proactive defensive programs that regularly evaluate high-valued employees whose backgrounds pose risks that cannot be discounted. Indeed, as the government’s Trusted Workforce 2.0 initiative institutes universal continuous evaluation of cleared personnel, such persistent monitoring will be the rule for everyone with a clearance.

Investigators and adjudicators are prone to bias—whether conscious or not—that could lead them to make assumptions about threats posed by candidates with foreign ties. They may instinctively treat a candidate with relatives in Belgium, for example, as inherently less risky than a candidate with relatives in Syria simply because of the state of U.S.-Belgian and U.S.-Syrian relations, or because of the greater terrorist threat emanating from Syria.⁶ Training on conscious and unconscious bias would help officials ensure thorough investigations and objective adjudications regardless of such conjectures.⁷

Cleared contracting firms that support intelligence agencies have important equities in this issue. Many companies have committed to increasing diversity in their workforce, both to advance social equity and to ensure their work products include diverse perspectives that lead to better analysis and decision-making. However, companies’ ability to hire workers who have foreign personal or family ties depends upon the government’s willingness to grant these employees clearances. If the government is unable to adjudicate an applicant’s foreign ties (or other issues) in a timely manner, the companies risk losing the employee to an organization that does not require a clearance—particularly in the science and engineering fields, in which commercial companies often hire faster and pay more than government agencies and cleared contractors. Therefore, for cleared industry to support its government clients effectively, the government’s clearance process must address foreign connections in a way that appropriately mitigates risk and provides prompt adjudication decisions.

SUCCESS REQUIRES A HUMAN RESOURCES AND CHIEF SECURITY OFFICER PARTNERSHIP

To increase the number of candidates in the pipeline who have global skills and experience, agencies human resources and security components must collaborate on recruiting and hiring initiatives designed to maximize diversity. Such opportunities could include:

- Career forums engaging university affinity groups
- Grants and scholarships for candidates with native-level foreign language skills
- Internships that bring candidates into the hiring and clearance pipeline well before graduation
- Enhanced campus outreach and education regarding intelligence careers by IC guest speakers
- The development and dissemination of instructional materials, aimed at students with interests in national security careers, on how to manage and minimize foreign influence

Security professionals must work with recruiters and others engaged in such outreach efforts to ensure they can accurately present the obstacles and opportunities presented by the clearance process. A recruiter's "best guess" as to how the security process would treat a candidate's foreign ties would do a disservice to the candidate, and potentially prolong an already lengthy process.

Once a candidate submits security paperwork that includes information on foreign ties, relatives, and travel, security offices begin their investigations but rarely engage the candidate right up front with a counterintelligence lens to request additional or clarifying information. Investigators often have difficulties gathering information about what a candidate did overseas, whom he/she engaged, and what his/her contacts' backgrounds are—particularly in developing countries or adversary nations where such investigative methods are difficult to employ.

In such cases, investigators often conclude they are unable to assess the candidate's foreign ties and activities and thus unable to mitigate the risk of foreign influence. In such cases, security officials should engage candidates and provide them opportunities to explain potential roadblocks and request clarifying information. An open dialogue that facilitates trust and transparent two-way communication can enable candidates to provide additional information to facilitate investigations or address security concerns.

Once a candidate's clearance is successfully adjudicated and a security clearance is issued, the now-cleared employee typically has little communication with the security office except for recurring training and the submission of required reports. Proactive and frequent outreach to employees with foreign ties would help create trust-based relationships that encourage employees to be transparent and forthcoming about developments in their foreign contacts and relationships. Such an approach is consistent with new Federal Personnel Vetting Engagement Guidelines approved by the DNI and Office of Personnel Management Director (as the Security and Suitability Executive Agents, respectively) in February 2022. These guidelines call on the vetting process to "benefit from transparent, open, honest, and frequent communication" and to "proactively communicate expectations and guidance to individuals as they progress through the personnel vetting process."⁸

DUAL CITIZENSHIP CAN BE A COMPLICATING FACTOR

Adjudicative guidelines note that dual citizenship is not itself disqualifying and consider factors such as the “low national security risk” of the foreign nationality to mitigate potential security concerns.⁹ Some federal agencies nevertheless maintain strict policies that an individual must renounce their foreign citizenship to be employed by that agency. Such a requirement may be unacceptable to someone who has no foreign preference but who nonetheless needs to keep dual citizenship to visit overseas relatives easily, own property, or ensure their children maintain access to future educational and employment opportunities. Unnecessarily requiring candidates to renounce foreign citizenship could deter highly skilled individuals from pursuing employment in the Intelligence Community. (As a counterintelligence matter, requiring a candidate to surrender their citizenship at a foreign embassy could attract scrutiny by a foreign security service and actually create a security risk for a new employee where none existed before.)

Security officials should fully assess the circumstances associated with applicants’ dual nationality through a detailed personal interview that explores not only the circumstances by which the candidate acquired citizenship, but also the reasons why the candidate may want to maintain it. Remaining risks may be mitigated by asking candidates to sign a binding agreement in which they commit to refrain from taking part in certain activities their foreign nationality may require or from exercising benefits it may confer. Compliance with such an agreement can be monitored by continuous evaluation and insider threat programs, as well as periodic re-attestations.



ACKNOWLEDGING AND CONFRONTING THE THREAT

Personnel with foreign connections are vulnerable to being targeted by foreign intelligence services. Security professionals must prepare these employees for this possibility. Such preparations must, over time, build a sufficiently strong sense of trust with employees so they feel able to report foreign approaches even if a foreign government threatens intensely personal repercussions for themselves and their family members. Employees are unlikely to volunteer information if they feel squeezed between a hostile foreign government and an intimidating, unsympathetic U.S. security apparatus.

Even as security officials work to build trust, they must also ensure that counterintelligence and insider threat tools are positioned to detect unreported foreign threats. Continuous vetting of trusted employees—which uses a range of data sources to identify potentially concerning behavior on an ongoing basis—can flag suspicious behaviors that employees do not voluntarily report. Counterintelligence polygraphs can be customized to explore the complex foreign ties of a candidate or employee with personal or family connections to a foreign country. By combining proactive outreach and traditional security tools, agencies can establish a positive, dynamic, and trusting relationship with higher risk employees, while continuously evaluating potential threats and vulnerabilities. As in arms control, trust but verify.

While government agencies are responsible for adjudicating clearances, both government agencies and cleared contractors monitor employees for behavior of concern during employment. Indeed,

“

As adjudicators learn lessons and identify best practices for mitigating risks associated with foreign preference, they should share their insights with industry so private companies can appropriately calibrate their insider threat methodologies.

the National Industrial Security Program Operating Manual (NISPOM), as revised in 2016, requires cleared contractors to establish and maintain programs to identify and mitigate insider threats.¹⁰ As adjudicators learn lessons and identify best practices for mitigating risks associated with foreign preference, they should share their insights with industry so private companies can appropriately calibrate their insider threat methodologies.

RECOMMENDATIONS

Agencies can take a range of steps to more responsively address risks and vulnerabilities associated with candidates with foreign ties.

- Security staffs should train recruitment teams on practices regarding applicants' foreign ties so clearance processes can be presented accurately to candidates for employment.
- Mission-focused teams—principally collectors and analysts—should identify “essential skills” necessary to fill mission-critical roles. They should work with human resources and security to ensure that candidates with such skills—which may include native-level language fluency and cultural proficiency—do not easily get dropped from the clearance process because of foreign ties. Investigators should take extra steps to ensure that the information needed to adjudicate a clearance for such candidates is gathered and considered.
- Agencies should provide bias awareness training—particularly extending to issues associated with ethnicity and national identity—to all officials responsible for recruitment, hiring, investigations, and adjudications.
- The Security Executive Agent, Suitability Security Agent, and all relevant stakeholders should review policies and procedures to ensure that their approach to mitigating risks from foreign ties is commensurate with the Intelligence Community's needs for critical skills.
 - > Review security forms to ensure candidates have ample opportunity to provide the data necessary to investigate foreign ties thoroughly. For example, simply requesting a foreign relative's or contact's name, address, date of birth, and employer name—as the SF-86 questionnaire for national security positions does—may not be sufficient to conduct a thorough assessment of the risk posed by the relative. Consider establishing a requirement for applicants to provide a biographical sketch, fully illuminating their foreign-born and immigration circumstances, foreign family members, foreign employment, ties to foreign governments, foreign assets, etc., to provide a baseline in the background investigation.
- > Review the Federal Investigative Standards and develop standard procedures for evaluating the importance and relevance of information gaps created by the inability to gather information overseas. If the Intelligence Community is to hire people with overseas experience, language skills, and cultural knowledge, the investigative process will need to identify measures to mitigate risks posed by such information gaps rather than deny clearances when such gaps exist.
- > Employ in-depth personal interviews to assess the reasons why candidates may wish to maintain dual citizenship and consider requiring that candidates sign binding agreements regarding the exercise of any benefits foreign nationality confers. Use continuous vetting and insider threat monitoring to confirm compliance.
- Direct that new employees with high-risk foreign ties receive in-depth security training and defensive counterintelligence briefings. Consider requiring such engagements at periodic intervals to ensure these employees are kept up-to-date on the tradecraft and tactics employed by relevant hostile nations.
- Agencies should periodically compile lessons learned and identify best practices for mitigating risks related to allegiance, foreign influence, and foreign preference.
- ODNI's National Counterintelligence and Security Center (NCSC), the Defense Counterintelligence and Security Agency (DCSA), and the Federal Bureau of Investigation (FBI) should periodically share lessons learned and best practices with industry so cleared contractors can effectively address foreign influence and foreign preference in their government-mandated insider threat programs.

CONCLUSION

A diverse workforce consisting of foreign-born U.S. citizens and individuals with international connections presents security and counterintelligence risks. However, it also provides the Intelligence Community with critical skill sets that enhance its performance and advance the national security mission. To take advantage of the skills these individuals possess, the IC must adjust its existing security and counterintelligence practices to ensure biases, presumptions, and unnecessary requirements do not deter candidates with foreign ties from applying for IC employment or needlessly prevent them from acquiring security clearances.

Innovative recruiting and vetting practices can identify, address, and mitigate challenges associated with personnel with foreign ties in the national security workforce. Success depends upon a shift from a risk-averse approach to a multi-layered strategy of ongoing risk management. A defensive strategy that pays special attention to candidates' foreign ties will enable the Intelligence Community to embrace a more diverse workforce that can contribute significantly to the national security mission.

REFERENCES

¹Office of the Director of National Intelligence, *Joint Strategy to Advance Equal Employment Opportunity, Diversity, and Inclusion Within the United States Intelligence Community 2020-2023*, August 2020. At https://www.dni.gov/files/EEOD/documents/2020-2023_IC_EEODI_Joint_Strategy_-_508.pdf.

²American Immigration Council, *"Immigrants in the United States,"* 2021. At https://www.americanimmigrationcouncil.org/sites/default/files/research/immigrants_in_the_united_states_0.pdf.

³National Science Foundation, *"Foreign-Born Students and Workers in the U.S. Science and Engineering Enterprise,"* National Science Board Science and Engineering Indicators 2020, no date. At <https://www.nsf.gov/nsb/sei/one-pagers/Foreign-Born.pdf>.

⁴Education Development Center, *STEM Smart Brief: Preparing Students for College and Careers in STEM*, March 22, 2013. At <https://successfulstemeducation.org/resources/preparing-students-college-and-careers-stem>.

⁵Security Executive Agent Directive 4 (SEAD-4), *National Security Adjudicative Guidelines*, June 8, 2017. At <https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf>.

⁶Adjudicative guidelines on foreign influence do require that "assessment of foreign contacts and interests should consider the country in which the foreign country or interest is located, including, but not limited to, considerations such as whether it is known to target U.S. citizens to obtain classified or sensitive information or is associated with a risk of terrorism." That said, individual adjudicators could have very different (and possibly ill-informed) views about the nature of country-specific counterintelligence and terrorism threats. Moreover, some countries are not monolithic. The U.S.-allied government of Iraq's Kurdistan region, for example, poses a lesser counterintelligence and terrorist threat than the political parties tied to Shi'a militias that predominate in the Iraqi capital of Baghdad; as a result, foreign contacts in the Kurdistan region may merit different consideration than those in the rest of the country. See SEAD-4, Guideline B: Foreign Influence.

⁷For insights on how organizations can identify and mitigate both conscious and unconscious bias in insider threat programs, see INSA, *Strategies for Addressing Bias in Insider Threat Programs*, January 2022. At <https://www.insaonline.org/wp-content/uploads/2022/01/Bias-and-Insider-Threat-Programs-Paper.pdf>.

⁸DNI Avril Haines and OPM Director Kiran Ahuja, *"Guidelines for Federal Personnel Vetting, Performance Management, and Engagement,"* Memorandum, February 10, 2022.

⁹See SEAD-4, Guideline C: Foreign Preference.

¹⁰See NISPOM, DoD 5220.22-M, rev. May 18, 2016, sec. 1-202. At <https://acqnotes.com/wp-content/uploads/2014/09/DoD-522022M-National-Industrial-Security-Program-Operating-Manual-NISPOM-18-May-2016.pdf>. See also Defense Security Service, *Industrial Security Letter ISL 2016-02*, rev. June 29, 2017. At <https://www.dcsa.mil/Portals/91/Documents/CTP/tools/ISL2016-02.pdf>.



**INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE**

ACKNOWLEDGEMENTS

INSA expresses its appreciation to the INSA members and staff who contributed their time, expertise, and resources to this paper.

INSA MEMBERS

Charlie Allen, *Chertoff Group; SPRC Chair*

Katherine Hibbs Pherson,
Pherson Associates; SPRC Vice Chair

Jim Onusko, *LexisNexis Special Services, Inc.*

Dennis Keith, *Leidos*

Chris Sharpley, *LexisNexis Special Services, Inc.*

Kylie Tokar, *Maxar*

Phil Mahoney, *Northrop Grumman Corporation*

Mary Rose McCaffrey,
Northrop Grumman Corporation

Michael Mullen

INSA STAFF

Suzanne Wilson Heckenberg, *President*

John Doyon, *Executive Vice President*

Larry Hanauer, *Vice President for Policy*

Peggy O'Connor, *Communications and Policy Director*

Rachel Thompson, *Fellow*

Nicholas Damianos, *Intern*

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit trade association dedicated to advancing collaborative, public-private approaches to intelligence and national security priorities. Through the application of industry expertise, leading-edge academic research and commercial best practices, INSA seeks to make the Intelligence Community more effective and efficient. Our 160+ member organizations and 4,000+ individual and associate members include senior executives and intelligence experts in the public, private and academic sectors.

ABOUT INSA'S SECURITY POLICY REFORM COUNCIL

INSA's Security Policy Reform Council seeks to transform the paradigms that govern the design and execution of security policy and programs and to serve as a thought leader on security issues. The Council works with industry and government stakeholders to identify and mitigate security challenges, develop security solutions, and advocate for security reforms to enhance industry's ability to support and protect national security.



INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

Building a Stronger Intelligence Community