**INTELLIGENCE INSIGHTS**
Expert Insights on
National Security Developments

July 2026

# Safeguarding National Security by Strengthening Identity Verification Procedures

*Presented by*
INSA'S INSIDER THREAT SUBCOMMITTEE

INSIDER THREAT SUBCOMMITTEE

## BACKGROUND

Federal identity assurance relies on established standards, including HSPD-12, FIPS 201-3, and OMB Memorandum M-19-17.[1] While these mandates provide a baseline for security, implementation across the broader national security and critical infrastructure ecosystem remains uneven. This fragmentation creates a significant security gap: while government agencies operate under rigorous, risk-based models, private sector partners lack a commensurate identity framework. While the cleared workforce is subject to rigorous federal vetting, a significant portion of support staff, including IT, finance, and administrative personnel, operates outside this high-assurance framework. This creates a security asymmetry, as these individuals possess privileged access to corporate networks and proprietary data, yet are not subject to the same national security-level scrutiny as their cleared counterparts.

The risks associated with a lack of standardization are further compounded by the fact that threat actors are increasingly utilizing synthetic identity fraud by combining legitimate data to create new, fictitious identities.[2] Certain schemes entail using stolen Social Security numbers, often belonging to a child, elderly, or deceased individual, that are then paired with a fake name, date of birth, and address.[3] Consequently, without more robust identity proofing standards in place, these actors are able to conceal their true identity, to include their actual geographic location, and successfully embed themselves within the U.S. workforce as legitimate employees.[4] These tactics could facilitate infiltration of critical networks, espionage, intelligence collection on high-value targets, sabotage, or other harmful activities.[5]

Additionally, recent cases illustrate that threat actors increasingly target specific industries, such as the information technology and engineering sectors, to gain access to sensitive data and steal intellectual property, including IP related to U.S. military technology.[6] Concerns are also growing with regard to U.S. citizens who may be recruited or paid to facilitate these scams on behalf of countries of concern.[7] And while there are no confirmed reports of individuals using synthetic identities to obtain security clearances, the likelihood that attempts could be made should be promptly addressed; identity proofing practices should not remain static and must be adapted to reflect the evolving threat environment. The resulting damage from imposters infiltrating other sectors critical to the national security ecosystem should be fair warning of the potential risks to our more sensitive government networks, where malicious actors could attempt to use similar tactics to work on classified programs.

To address these challenges, this paper proposes the creation of a Joint Identity Management and Security Working Group, led by DCSA, to adapt existing federal models, calibrated by risk, cost, and operational reality to strengthen our industrial base against modern social engineering threats and growing risk of synthetic identity.

## PART I: IDENTITY ASSURANCE CHALLENGES

This section examines the challenge of addressing the first primary risk area where we examine the challenge of verifying an individual's identity during the initial hiring and proofing process. This phase is critical to ensuring that the person applying for a role is indeed the person they claim to be, thereby preventing the infiltration of false identities into sensitive environments.

### MODERNIZING IDENTITY VERIFICATION WITH BIOMETRIC AND BIOGRAPHICAL DATA

Verifying one's identity using biometric and biographical data has become commonplace. Daily, we hold our phones up to our faces or hold our thumbs on a sensor to unlock our devices. Common types of biometrics for identity verification are facial recognition, fingerprint scanning, voice recognition or voice analysis, behavioral biometrics (such as keystrokes), iris recognition, and vein recognition.[8] Similarly, it is also commonplace, and especially for hiring purposes, to verify one's identity using primary or secondary identification documents to prove a person is who they claim to be.

Primary fixed or static documents include valid government-issued IDs, such as a driver's license, state ID card, passport, military ID, or permanent resident card (e.g. Green Card).[9] Secondary supporting identification documents include a Social Security card and birth certificate.[10] Generally, most forms of ID feature a photograph of the holder and a unique identification number, such as a driver's license number or passport number.[11] Ultimately, with respect to identity verification, the assumption is when a person submits one or more copies of identification documents, that person is *the* person – a real person – depicted in the photo and legitimately affiliated with the unique number. However, this is not always the case.

To better detect whether an identity may be fraudulent, talent acquisition specialists and security personnel should layer biographical data with other available data when reviewing a candidate's information. For example, core biographical data elements are routinely collected during the initial application process or background checks, such as full name, home address, date of birth, and Social Security number. Those elements, when added to digital markers, such as email address, phone number, and if applicable, an IP address, could be used to perform a "history check" to determine if an identity has a "real" history. A "real" history implies a digital marker has existed for a period of time, whereas those that were recently created should be flagged for further review. Staff could note whether a phone number or IP address associated with a device that was used to submit information are less than 30 days old. A home address can also be crosschecked against a phone number to verify if the two are associated. By overlaying biometric data with biographical data, hiring agents could further narrow the opportunity for a bad actor to bypass vetting procedures if other means of identity verification fail during the hiring process.

## CRITICAL VULNERABILITIES IN IDENTITY VERIFICATION

U.S. government departments and agencies rely on a combination of documentary and biometric identity verification procedures that function as required components to the hiring process and are executed prior to extending formal offers of employment or issuing certain credentials, such as PIV or CAC cards.[12] For fingerprinting specifically, FIPS 201-3 requires agencies to ensure that "the individual who appears for identity proofing and whose fingerprints are checked against databases is the person to whom the credential is issued."[13] However, under FIPS 201-3, biometric identification using fingerprints is described as "the primary input to law enforcement checks," meaning prints are likely collected to verify whether the individual has a criminal record, is on probation, or has a history of certain police actions, among other things.[14] If an individual has a record, one could assume certain information logged in a government system would match information submitted by that person during the hiring process. However, what if the individual does not have a record? As no two persons can have the same fingerprints, it is worth exploring options to use this type of biometric data to support identity proofing in addition to law enforcement checks to strengthen existing policy.

By comparison, some private sector and quasi-governmental entities, including cleared government contractors, may follow the FIPS standards but most commercial hiring practices rely on key data submitted by candidates on required forms instead of biometric data or other enhanced procedures to confirm "true identity." However, organizations remain vulnerable to internal 'soft targets'—unvetted employees in back-office roles who maintain administrative control over enterprise systems. These positions often lack the enhanced scrutiny applied to cleared staff, despite the reality that an adversary who compromises an unvetted account can secure a foothold to exfiltrate intellectual property or disrupt critical supply chains. This can be especially true for remote positions, where more stringent practices may be deemed unnecessary or cost prohibitive, which in turn could leave existing processes lacking in substance or create gaps that could be identified and exploited by a bad actor.

For instance, the I-9 Form is used by companies to verify that a candidate is authorized to work in the U.S. The form requires newly-hired staff to submit copies of multiple types of documents, such as a valid driver's license, U.S. passport, or birth certificate.[15] Although information pulled from those documents is supposed to be verified using certain systems such as E-Verify, there is no further requirement to definitively confirm if the photo associated with a driver's license or passport was manipulated, AI-generated, or replaced with a different photo if the credentials are otherwise valid.[16] In other words, E-Verify stops short at requiring that the photo on an ID be compared against other official records. That said, for virtual interactions, E-Verify does provide an "Alternative Procedure to Physical Examination" where an employer "in good standing" can conduct a live video call with an applicant to "ensure the documentation reasonably appears to be genuine and relates to the individual."[17] Here, "reasonably appears to be genuine" is subjective at best and the language fails to require that the person on the video call "reasonably appear" to be a live person versus an image manipulated by AI for the purposes of the video interaction. Further, the I-9 instructions allow employers to hire an authorized agent of their choosing to "examine the documentation [the] employee presents, complete Section 2, sign and date the form" and without any additional proof they complied with said instructions. Moreover, an "authorized representative" could be anyone, including an individual acting in concert with an employer, to fraudulently sign off on the I-9 form.[18]

The risk extends beyond the commercial sector. Identity fraud schemes will continue to evolve along with increasingly sophisticated AI and other identity spoofing capabilities. All critical infrastructure organizations – including utilities, transportation, healthcare, biotechnology, energy, and scientific research – are vulnerable. Despite comprehensive identity verification requirements, even the public sector and cleared industry may be vulnerable to exploitation, especially with respect to remote workers; and remote work is not just a legacy of the Covid-19 pandemic, but a cost saving and efficient way to meet mission needs and recruit talent beyond the confines of a specific geographic area. To fully support the reality of the modern workforce, robust identity verification standards must be continuously enforced but also dynamic to account for new tactics used by adversaries to try to pose as legitimate employees or contractors to gain access to FCI, CUI, and remote government workspaces.

**Personnel Vetting:** The process by which a person's background, character, suitability, and trustworthiness to hold certain positions are investigated, evaluated, and adjudicated. Vetting is governed by several authorities, such as E.O. 13467.[19]

**Credentialing:** The technical process of verifying identity and issuing access credentials (e.g., PIV/CAC), governed by standards such as FIPS 201-3.[20]

**Work Authorization and Background Screening:** To include processing the I-9 form and performing employment and education verification and reference checks.

## NATIONAL SECURITY IMPLICATIONS OF IDENTITY FRAUD

The U.S. government depends on identity verification procedures to ensure that candidates applying to any job are not misrepresenting themselves. This becomes even more critical for people hired in positions of trust. While most existing standards provide significant safeguards, malicious actors may attempt to undermine those processes nonetheless. Evaluating that risk is urgent; imposters in the private sector have gained access to sensitive systems to steal intellectual property. This threat has the potential to extend across critical infrastructure sectors including state and local governments, utilities, Industrial Control Systems, and other sensitive programs or operations across the U.S. – including those in federal departments and agencies.

All organizations must be able to definitively confirm the identity of potential employees. Consequences for private sector and quasi-governmental organizations for not doing so may include legal liability, financial penalties, government investigations, contract terminations, and reputational harm. For government agencies, the consequences may range from operational disruption to strategic compromise, cyber incidents, and fraud. Of note, identity validation vulnerabilities have also extended beyond the workforce. A recent False Claims Act settlement indicated Chinese-owned companies were able to take advantage of U.S. financial assistance programs by obtaining loans they were not otherwise eligible for.[21] The amount of fraud related to bad actors exploiting weak verification processes has clearly increased over time, which serves as yet another example of how critical it is that the procedures related to verifying any type of identity – whether that of an entity or individual – requires attention to better protect U.S. programs, taxpayer dollars, and ultimately, our national security.[22]

## KEY RECOMMENDATIONS

### ESTABLISHMENT OF A JOINT IDENTITY MANAGEMENT & SECURITY WORKING GROUP *(45 DAYS)*

DCSA should establish a Joint Identity Management & Security Working Group comprised of industry partners, academic institutions, and government stakeholders, including CISA, OPM, OMB, DHS, and NIST. This group will synthesize current government identity requirements into a modular, scalable framework that allows organizations of any size to adopt high-assurance verification standards. By aligning with the risk-adaptive principles set forth in OMB Memorandum M-19-17, this framework will help the industrial base modernize its security posture while managing implementation costs. Additionally, the group will identify the executive, legislative, or regulatory actions necessary to support broader, voluntary adoption of these standards across the industrial base.

The working group should focus on the following practical outcomes:

Remote Hiring: Adapting government frameworks to better meet commercial needs.

Vetting Strategy for Non-Cleared Staff: Developing a risk-based methodology, in coordination with CISA and DIB stakeholders, for organizations to identify high-impact non-cleared roles (those with privileged access to enterprise networks, financial systems, or sensitive data) and apply high-assurance identity verification commensurate with that access.

Fraud Detection: Developing guidance for detecting synthetic and fraudulent identities, both pre- and post-hire, to close gaps currently exploited by adversaries.

Threat Sharing: Establishing a feasibility study for an official forum where government and industry can securely share real-time identity threat indicators, structured to mimic trusted services like the NSA's Cybersecurity Collaboration Center and DHS's Homeland Security Information Network.[23]

### CONDUCT GOVERNMENT/INDUSTRY STUDY *(60 DAYS)*

For maximum engagement, the task force could conduct a review of existing policies and procedures to better understand the processes and best practices for verifying the identity of prospective employees across the public and private sector.[24] The study could also request participants to detail any technologies used to support or expedite the identity verification process.

## PART II: CREDENTIAL AND ACCESS PROTECTION INITIAL FINDINGS & RECOMMENDATIONS *(90 DAYS)*

The task force should compile a report detailing initial findings, recommendations, and next steps. Reports should be made available to the public to encourage comment and feedback. Recommendations could reflect the following:

– Standardize Biometric Use into Pre-Employment Vetting Procedures

The working group should establish a standard requiring the integration of biometric data, such as fingerprints, facial recognition, or voice analytics, as well as device history checks, into pre-employment vetting for sensitive roles to mitigate the risk of AI-generated credential manipulation. This will assist with definitively verifying the identity of candidates applying for roles that require a security clearance, Public Trust designation, or any remote work that requires access to sensitive systems.

Biometric verification should also be used to detect if candidates are using AI to manipulate an onscreen image or voice during live, virtual interviews. Further, hiring agents tasked with processing I-9 documents should also be encouraged to confirm that photographs from a driver's license or passport are not AI-generated and can be attributed to the actual candidate using other trusted sources such as the Department of Motor Vehicles (DMV) or other government repositories authorized to share certain PII.

Biographical data should also be continuously connected to the identity of the candidate throughout the entirety of the process. Address or phone number changes or suspect device history checks that do not align with the biometrics identity resolution process should be flagged for further review.

– Strengthen Remote Form I-9 Examination and Authorized Representative Controls

The appropriate federal authorities should revisit Form I-9 instructions governing the use of authorized representatives and the remote examination of identity and employment authorization documents. This review should assess whether current procedures provide sufficient safeguards against fraudulent documents, synthetic identities, manipulated images or video, and the use of complicit or inadequately trained third parties. The review should consider whether additional guardrails are needed to strengthen employer oversight and accountability, confirm that documents relate to the individual presenting them, and document and escalate inconsistencies or indicators of suspected fraud. Additional considerations may include training, attestation, recordkeeping, and audit requirements for authorized representatives. This review is particularly critical for non-cleared staff in high-impact roles, where the absence of federal background investigations makes robust, internal identity proofing the primary defense against infiltration.

– Adopt a Continuous Identity Verification System

Identity verification should not end after hiring or credential issuance. Government agencies and organizations should adopt continuous identity verification procedures to periodically confirm that individuals accessing facilities, systems, and sensitive information remain the authorized users associated with their identities and access privileges.[25] Additionally, occasional reverification of employment and income records could assist with identifying overlapping employment data, which may reveal that an employee's identity has been unknowingly stolen or intentionally sold for the purposes of enabling hiring schemes.[26] Generally, identity verification checkpoints should be conducted periodically, at random, or in response to defined risk indicators. These checkpoints could use one or more forms of biometric verification, secure video authentication, or other identity assurance measures appropriate to the sensitivity of the position and level of access. Access to facilities or secure networks should be temporarily restricted when an individual's identity cannot be confirmed, pending further review.

– Modernizing Identity Assurance for High-Impact Roles and Positions of Trust

Identity assurance should not end at the point of hire, and it should not be limited to positions requiring a clearance. Organizations should extend identity proofing and periodic reverification to non-cleared employees whose roles carry privileged access to financial systems, source code, or network infrastructure, calibrating the level of assurance to the sensitivity of that access rather than to clearance status alone. A back-office employee with administrative control over enterprise systems can pose the same operational risk as a cleared employee with access to classified information, even though current practice treats the two very differently.

The working group should not prescribe a single required technology. Instead, it should establish that organizations confirm identity at hiring commensurate with the access being granted, reconfirm that identity periodically throughout employment, and restrict or suspend access when identity cannot be confirmed, consistent with the risk-adaptive, cost-conscious approach already adopted under OMB Memorandum M-19-17.
Baseline requirements should also address monitoring and reporting of unauthorized credential sharing and prompt investigation of suspected unauthorized use, with defined procedures for rapid suspension or revocation when identity cannot be verified. The specific tools used to meet these outcomes should remain at organizations' discretion.

– Implement Additional Identity Verification Requirements for Remote Logins

  Identity verification using biometric data should be the standard not the exception for any remote login. Requiring multi-factor biometric authentication, such as a combination of fingerprints and facial recognition or voice analytics, could prevent unauthorized individuals from using another person's credentials or flag an individual that may have successfully circumvented identity verification procedures during the initial hiring process.

  Also, whether multiple types of biometric data should be used could be based on assigned level of privilege, where it may be more appropriate to require three or more types of biometric data to gain access to systems storing highly sensitive or classified information. Further, both agencies and organizations should consider using secure video authentication for periodic identity checks of remote employees in sensitive roles. These measures could reduce opportunities for imposters to operate undetected in remote environments without allocating significant resources to implement cost-prohibitive solutions or creating unnecessary administrative tasks.

– Ensure NBIS and Continuous Vetting Processes Support Identity Verification Using Biometric Data

  As the transition to the National Background Investigation Services (NBIS) and Trusted Workforce 2.0 (TW 2.0) continue, it will be essential to ensure these initiatives support integrating identity verification procedures using biometric data throughout the investigative workflow and beyond. Piloting various methods and technologies to identify challenges before full scale adoption will be critical to successful implementation to minimize disruption.

– Provide Guidance to Promote Consistent Enforcement and Encourage Implementing Continuous Employee Awareness and Training Programs

  Policies and their corresponding internal controls serve no purpose unless all staff, regardless of seniority, demonstrate their commitment to protecting their domain. This is accomplished not only by setting a consistent example but by properly implementing procedures, communicating new guidelines across the organization, and consistently enforcing policy. Similarly, employees who actively participate in continuous training and awareness programs are more likely to adhere to policy if they understand the purpose behind them and the consequences for failing to comply. When personnel understand that adversaries are actively targeting unvetted back-office staff to exploit corporate networks, vigilance will increase, significantly reducing the likelihood that imposters can blend into a trusted environment.

  Examples of guidance include developing standards for monitoring unauthorized credential sharing, informational bulletins on the risks of identity schemes, annual training for identifying indicators of insider risk specific to hiring fraud, and suggestions on how to incorporate hiring fraud awareness campaigns to Insider Threat Programs to help encourage safe and secure reporting of potential incidents through proper channels. At a minimum, training should include human resources professionals, security personnel and investigators, management, and other employees as appropriate.

## JOINT TASK FORCE STUDY – ADDITIONAL CONSIDERATIONS

– Should resources be allocated to support information campaigns to better inform industry and the public at large on how to safely and securely report concerns or share information with the government concerning incidents related to hiring fraud?

– Which government agency is responsible for issuing public alerts or bulletins based on information shared or reported? Are those alerts effective in reaching as many individuals, organizations, and government agencies as possible?

– Consider requesting copies of internal policies and procedures or other existing frameworks from select government entities to compare internal controls or guidelines to identify best practices, baseline standards, and performance metrics as applicable.

– Consider requesting the same from participating industry partners to identify commercial best practices and baseline standards as well as cost and pricing data to evaluate the resources needed to implement identity verification programs for organizations of any size, from sole proprietorships to large corporations.

– What other technologies are commercially available to support identity verification in the hiring lifecycle?

– Determine the risks of third parties contracted to perform personnel vetting or background investigations or screenings on behalf of both government agencies and organizations and develop recommendations to ensure identity verification is included with scopes of services.

– Ensure task force conversations emphasize the importance and value of using both biographical background investigations and biometric data in identity verification as it concerns the pre/post hiring process.

## CONCLUSION

Hiring schemes involving identity fraud pose an immediate threat to national security and the integrity of the U.S. workforce. Ensuring – where possible – that identity verification procedures use overlaying biometric data with biographical data in addition to identity proofing best practices will significantly reduce the risk of imposters gaining physical or logical access to critical systems, intellectual property, or sensitive government networks.

Biometric technology already exists, and many private sector organizations have already adopted measures that may already align with FIPS 201-3 and HSPD-12. However, implementation is not standardized across the broader national security and critical infrastructure ecosystem and application of best practices in a rapidly evolving technology environment is challenging. The necessary next step is to establish a Joint Identity Management & Security Working Group led by DCSA to synthesize federal requirements into a modular, scalable framework.

By strengthening identity verification procedures, both government and industry will better safeguard critical assets, reinforce trust in the hiring and personnel vetting processes, and prevent adversaries from further exploiting weaknesses in the identity verification infrastructure. Addressing these vulnerabilities now by applying a whole-of-nation approach to defend forward, will protect both national security and the workforce entrusted with defending it.

## *REFERENCES*


1 See https://www.dhs.gov/homeland-security-presidential-directive-12, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-3.pdf, and https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf.

2 See https://www.transunion.com/blog/what-is-synthetic-identity-fraud and https://oig.hhs.gov/documents/root/9990/ OEI-07-22-00510-highlights.pdf.

3 https://www.gao.gov/products/gao-20-492.

4 See https://www.justice.gov/opa/pr/justice-department-announces-nationwide-actions-combat-illicit-north-korean-government and https:// sessions.house.gov/2026/1/ongressman-pete-sessions-introducesbipartisan-legislation-to-combat-identity-fraud-and-theft.

5 https://www.justice.gov/usao-ma/pr/new-jersey-man-pleads-guilty-participating-scheme-generate-revenue-north-korean-weapons.

6 See https://www.crowell.com/en/insights/client-alerts/from-deepfakes-to-sanctions-violations-the-rise-of-north-korean-remote-it-worker-schemes and https://www.justice.gov/opa/pr/ justice-department-announcesnationwide-actions-combat-illicit-north-korean-government.

7 *Id.*

8 See https://www.abiresearch.com/blog/types-of-biometrics and https://id4d.worldbank.org/guide/biometric-data.

9 See https://faq.usps.com/s/article/Acceptable-Form-of-Identification and https://help.id.me/hc/en-us/articles/360017833054-Primary-andsecondary-identification-documents.

10 *Id.*

11 *Id.*

12 See https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-3.pdf, https://www.cac.mil/Common-Access-Card/Getting-Your-CAC/, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-79-2.pdf, and https://www.dhs.gov/homeland-security-presidential-directive-12.

13 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-3.pdf.

14 *Id.*

15 https://www.uscis.gov/sites/default/files/document/forms/i-9instr.pdf.

16 https://www.e-verify.gov/employees/e-verify-overview.

17 https://www.uscis.gov/i-9-central/remote-examination-of-documents.

18 https://www.uscis.gov/i-9-central/completing-form-i-9/completing-section-2-employer-review-and-attestation.

19 See https://www.dni.gov/files/NCSC/documents/Regulations/EO_10450.pdf, https://www.dni.gov/files/NCSC/documents/Regulations/EO_13467.pdf, https://www.govinfo.gov/content/pkg/FR-2017-01-23/pdf/2017-01623.pdf, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520002m.pdf, and https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf.

20 See https://www.dhs.gov/homeland-security-presidential-directive-12, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-3.pdf, and https://www.cac.mil/Common-Access-Card/Getting-Your-CAC/.

21 See https://www.gao.gov/products/gao-25-107753, https://www.gao. gov/products/gao-24-105833, and https://www.justice.gov/opa/pr/ three-chinese-owned-companies-pay-more-73m-resolve-false-claimsact-allegations-relating.

22 See https://fedgovtoday.com/guests/fraud-at-the-front-door-why-government-must-rethink-identity-verification-now.

23 See https://www.nsa.gov/About/ Cybersecurity-Collaboration-Center/ and https://www.dhs.gov/homeland-securityinformation-network-hsin.

24 U.S. state biometric privacy legislation may also provide valuable insight into current regulations concerning collection and use of biometric information. For an example of certain state legislation, see https:// www.huschblackwell.com/2024-state-biometric-privacy-law-tracker.

25 https://www.cisa.gov/topics/cybersecurity-best-practices/ zero-trust.

26 See https://theworknumber.com/how-it-works, https://www.dol.gov/agencies/oasam/ centers-offices/human-resources-center/employment-verification, https://www.justice. gov/usao-sdga/pr/three-sentenced-facilitating-computer-access-northkorean-sanctions-evasion-scheme.

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*

Michael Crouse, *Chair, Insider Threat Subcommittee*

Theresa Campobasso, *Vice Chair, Insider Threat Subcommittee*

Lorna Macfarlane

Donald Blersch, *Defense & Security Advisor, Clearspeed Inc.*

Michael Hudson, *Vice President, ClearForce*

Gregory Torres, *Director, Booz Allen Hamilton*

Michael Whalen, *Vice President, Ideal Innovations, Inc.*

### *INSA STAFF*

Suzanne Wilson Heckenberg, *President*

John Doyon, *Executive Vice President*

Peggy O'Connor,
*Senior Director of Communications and Policy*

Nicole Leung, *Marketing & Communications Manager*

Stephanie Bulega-Nasuna, *Policy Intern*


---

## ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit membership organization 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 180 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 INSIDER THREAT SUBCOMMITTEE

INSA's Insider Threat Subcommittee researches, discusses, analyzes, and assesses counterintelligence and insider threat issues that affect government agencies, cleared contractors, and other public and private sector organizations. The Subcommittee works to enhance the effectiveness, efficiency, and security of government agencies and their industry partners, as well as to foster more effective and secure partnerships between the public, private, and academic sectors.