



June 18-19, 2019
Mary M. Gates Learning Center, Alexandria, VA

IDENTITY MANAGEMENT SYMPOSIUM

LEVERAGING IDENTITY INTELLIGENCE AND BIOMETRIC CAPABILITIES TO ENHANCE NATIONAL SECURITY



“Leveraging Identity Intelligence and Biometric Capabilities to Enhance National Security”

June 18, 2019

8:00—8:45	Registration and Light Breakfast Reception Open
8:45—9:00	Moderator Opening Remarks Moderator: Douglas Lindquist, Assistant Director, FBI CJIS (ret.)
9:00— 9:45	Advancing DoD Identity Intelligence Capabilities through Policy and Strategy Development <ul style="list-style-type: none">• Overview of USD(I) current identity intelligence, biometrics, and forensics programs and initiatives—how do these programs boost mission success?• Working with stakeholders, IC components, and interagency partners to increase USD(I) identity intelligence capabilities—how can these partnerships be strengthened? Where is there a need for industry to get involved?• Looking towards the future—how will technology advancement, doctrine development, and policy effect the evolution of identity intelligence? Christopher Munn, Chief of Identity Intelligence, Under Secretary of Defense for Intelligence (Confirmed)
9:45—10:30	Criminal Justice Information: How CJIS Uses Identity Data to Stop Crime <ul style="list-style-type: none">• CJIS and the FBI's role as the keeper of the nation's criminal justice information—how will this role continue to evolve as technology and policy changes?• How has the role of biometric data evolved from the creation of the Identification Division's collection of fingerprints in 1924 to today?• The intersection between equipping partner agencies with necessary criminal justice information and preserving civil liberties—what are the difficulties? Will the new Clarksburg campus developed with the Army make information sharing easier? Section Chief Scott Rago, Global Law Enforcement Support Section, CJIS, FBI (Confirmed)
10:30—10:45	Networking Break
10:45—11:15	Duo Tech Talk
11:15—12:00	Coordinating Inter-Agency Identity Intelligence to Prevent Threats to National Security <ul style="list-style-type: none">• Overview of the newly-established National Vetting Center—what is the Center's role in vetting threats against the United States?• Thoughts on the role of biometric, forensic, and identity intelligence in threat detection and prevention• Current challenges faced by the NVC—what are the policy and technology barriers obstructing progress and how can we overcome them? Casie Antalis, Chief of Staff, National Vetting Center, DHS (Confirmed)
12:00—12:45	Leveraging Biometrics for Threat Detection and Defense <ul style="list-style-type: none">• Overview of DFBA's role in leading, consolidating, and coordinating DoD biometric capabilities in support of identification activities• The role of the DoD ABIS in OCONUS operations and national security—How can we use identity management to its maximum potential on the battlefield?• Intelligence sharing and coordination between DFBA and its domestic and foreign partners—how can this be improved? Glenn D. Krizay, Director, Defense Forensics and Biometrics Agency (DFBA) (Confirmed)
12:45—1:30	Networking Lunch

1:30— 2:15	<p>Identity Dominance for the Warfighter and Across the Department of Defense</p> <ul style="list-style-type: none"> • Provide updates on current programs including ABIS, BAT-A, and the Biometric System Integration Lab and their future considerations • Challenges and considerations for acquisition—how to balance requirements with affordability and technological longevity? Where can industry help PEO IEW&S meet its goals? <p>William Graves, Chief Engineer, PM DoD Biometrics, PEO IEW&S, Department of Defense (Confirmed)</p>
2:15—3:00	<p>Advancing the State of Identity Management in Immigration</p> <ul style="list-style-type: none"> • Implementing biometric data collection, analysis, and processing systems like ELIS to reduce fraud in immigration applications and increase processing speed and efficiency • The policy aspect of biometrics—describe the process of obtaining formal rules for USCIS usage of voice, iris, and rapid DNA identification? Did USCIS reach its stated goal of March 2019? <p>Lee Bowes, Deputy Associate Director, Immigration Records and Identity Services Directorate (IRIS), US Citizenship and Immigration Services (Confirmed)</p>
3:00—3:30	<p style="text-align: center;">Networking Break</p>
3:30—4:15	<p>Mitigating Adversaries' Anonymity through Identity Operations</p> <ul style="list-style-type: none"> • Challenges posed by anonymity of adversaries in complex terrain operational environments—how can identity intelligence give back the advantage to the Marine? • World-wide data management capability—how to ensure the ability of the Marine to submit and access database information from any environment? • Looking toward the future—how will evolving technologies and shifting policies impact the Marine Corps' identity operations? What effect will this have on operational flexibility and mission success? <p>Jeremy Powell, Identity Operations Manager, HQMC (Confirmed)</p>
4:15—5:00	<p>Securing Points of Entry through Identity Management</p> <ul style="list-style-type: none"> • Overview of CBP's Entry/Exit program and the Traveler Verification Service (TVS)—how does this program help predict and prevent threats to national security and transportation? • Data storage and access—is the current cloud-based storage system here to stay? What are the pros and cons of the cloud? • Navigating privacy and civil liberty concerns as data collection capabilities evolve-what are the current and future challenges? What was found by the 2018 Privacy Impact Assessment? <p>Michael Hardin, Director of Policy and Planning, Entry/Exit Program Office, CBP (Invited)</p>
5:00—5:45	<p>Research Spotlight: The Future of Biometric Identity Intelligence</p> <ul style="list-style-type: none"> • Thoughts on the implications of biometric identity intelligence developments • Overview of person-centric identity work at RAND • Looking to the future: how will our capabilities evolve alongside developing technologies? <p>Dan Gonzales, Senior Scientist, RAND (Tentatively Confirmed)</p>
5:45	<p style="text-align: center;">End of Day One</p>

8:15—8:45	Registration and Light Breakfast Reception Open
8:45—9:00	Moderator Opening Remarks Moderator: Douglas Lindquist, Assistant Director, FBI CJIS (ret.)
9:00—9:45	Leveraging Biometric Identification for National Security <ul style="list-style-type: none"> • Data centralization: How does OBIM act as a gatekeeper of government biometric data through programs like IDENT and now HART? What is the policy on sharing this information with partner organizations? • Overview of non-permissive biometric identification—how can technologies like facial recognition, gait recognition, latent fingerprinting, eye tracking, etc. assist in identification? How can they increase the efficiency and security of access management? • Looking towards the future—where is the field of biometrics headed? What will be the biggest challenges to collecting, analyzing, and implementing this data? Shonnie Lyon, Director, Office of Biometric Identity Management (OBIM), DHS (Confirmed)
9:45—10:30	Revolutionizing the Creation and Management of Digital Identities through Innovation <ul style="list-style-type: none"> • Overview of the role of DoD CIO and how it works with DISA, DMDC, NSA and other intelligence partners • Thoughts on the role of CAC cards in DoD access management and how this will evolve alongside new technologies • Leveraging ICAM to protect DoD against outside hacks and insider threats Colonel Tom Clancy, IdAM Lead, CIO, Department of Defense (Confirmed)
10:30—11:00	Networking Break
11:00—12:30	Panel Discussion: Leveraging Identity and Access Management to Prevent Insider Threats <i>This panel will convene experts from federal government and academia to discuss the ways in which Identity and Access Management can be utilized to predict and prevent insider threats. Panelists will provide delegates with insights into the various potential threats posed by insiders, new developments in the technology driving IAM and the applications of this technology, and how to use IAM to reduce the risk of employee-related information loss and security breaches.</i> Moderator: Daniel Costa, Technical Manager, Insider Threat Center, CERT, Software Engineering Institute, Carnegie Mellon University (Invited) Panelists: JT Mendoza, Deputy Director, USAF Insider Threat Hub (Confirmed) Dave Paravecchia, Director, US Army Insider Threat Hub (Tentatively Confirmed) Brian McGill, Director of Threat Management, Pentagon Force Protection Agency (Tentatively Confirmed)
12:30—1:20	Networking Lunch
1:20—2:05	The Future of Facial Recognition Technology <ul style="list-style-type: none"> • Overview of current facial recognition research and developments at NIST—case study of FVRT 2018 • What are the greatest challenges to facial recognition technology? Do these challenges fall mainly on the side of data collection or data analysis? How are these challenges being mitigated? • The future of facial recognition—what role will machine learning play in the evolution of facial recognition? How will the technology be used in the future? How do you see the technology evolving? Patrick Grother, Biometrics Standards and Testing Lead, NIST (Confirmed)

2:05—2:15	<p>Tech Talk: Identity Virtualization as a Means for Leveraging Existing Assets for Future Initiatives</p> <ul style="list-style-type: none"> • Abstracting and virtualizing existing identity systems to more flexibly support mission critical applications • Highlighting how identity virtualization can change the game for enterprises with significant investments in legacy systems while also adapting these systems for future applications <p>Esteban Soto, Senior Solutions Architect, Radiant Logic (Confirmed)</p>
2:15—3:00	<p>The Data of Defense: Providing the Right Information to the Right People at the Right Time</p> <ul style="list-style-type: none"> • Overview of the DMDC's mission—what role does DMDC serve within the DoD? How has this role changed over time, and how will it continue to evolve? • Thoughts on the future of data storage and management—what would make this more efficient and secure? • Intelligence sharing—how can DMDC better collect, analyze, and share data with its partners? <p>Denise McFaddin, DMDC - Identity, Credential and Access Management (Confirmed)</p>
3:00—3:45	<p>Gathering and Sharing Intelligence to Counter the Terrorist Threat</p> <ul style="list-style-type: none"> • What role does biometric data play in the Terrorist Screening Database? How will this evolve as new technologies are developed? • How can identity management technologies be leveraged to anticipate and prevent extremist threats? • Thoughts on the challenges of information sharing—what are the policy and technology constraints that make inter-agency information exchanges difficult? <p>Identity Intelligence Unit, Terrorist Screening Center, FBI (Confirmed)</p>
4:00	<p style="text-align: center;">End of Symposium</p>