COVID-19 Surveillance:
Hidden Risks and Benefits for Identity Intelligence

Photo collage by the National Ground Intelligence Center

by Ms. Christine Kaiser, Mr. Gregory Smith, and Mr. Kasey Diedrich

The views expressed in this article are those of the authors and do not necessarily reflect the official policy or position of the Departments of the Army or Defense, or the U.S. Government. This article does not imply nor should the reader infer the policies and regulations covering intelligence oversight have changed. Intelligence activities must comply with and adhere to applicable law and policies pertaining to the collection of publicly available information and U.S. person data. These include, but are not limited to, Executive Order 12333, the Foreign Intelligence Surveillance Act, DoD Manual 5240.01, and AR 381-10.

Identity intelligence is "the analysis and fusion of human signatures with other information concerning individuals, entities, groups, networks, or populations of interest to identify intent, actions, and activities for validation during the assessment."

—Identity Intelligence Concept of Operation

Introduction

Just as Galileo's first crude telescopes resolved the light of distant celestial bodies, a new generation of tools is enabling the world to distinguish previously uncollectible and indiscernible human signatures. By fusing diverse data sets and taking advantage of rapidly improving new technologies, identity intelligence (I2) promises to offer ever-clearer insights into the human mosaic, including in public, private, military, and civilian sectors. However, the advent of artificial intelligence-enabled biometrics, big data, increased computing power, and worldwide crises, such as the coronavirus disease 2019 (COVID-19) pandemic, is driving exponential growth in personal data production, data capture ability, and data fusion using machine-aided analytic systems. Worldwide COVID-19 is forcing human activity to accelerate online, generating increased personal and professional digital interaction from which useful patterns can be discerned. In the competition phase of multi-domain operations, the troves of I2 data generated from our digital footprints can highlight patterns of movement, military planning, and key individuals, providing immense value to friends or foes with mature I2 capabilities. Conversely, I2 with foreign datasets can assist U.S. commanders in understanding and better identifying the human aspect of the operational environment across all physical domains (air, land, maritime, space, and cyberspace) and within the information environment. As the Army transitions away from counterinsurgency-centric operations and postures for future large-scale ground combat operations against peer/near-peer nation states, the military force that can access foreign I2 data and best use I2 tools will have a distinct advantage in more fully understanding the operational environment, and thus be able to more effectively employ capabilities on the battlefield.

Background

An article in the January–March 2020 *Military Intelligence Professional Bulletin,* titled "Identity Intelligence Contributes to Multi-Domain Operations," examined how I2 can support multi-domain operations across all of its phases, including competition, armed conflict, and return to competition.[1] We continue the I2 theme in this article by highlighting the increasing global availability of and interest in I2 data, which is a fusion of biometric, biographical, and behavioral attributes that can provide powerful analytic insights at micro- and macroscales. In all multi-domain operations phases, I2 can support the identification of persons of military interest, and their intent, by distinguishing individuals from each other; discovering new threats; linking individuals and threats to other people, places, things, actions, and activities; and properly characterizing individuals, entities, groups, networks, and populations of interest. In the conflict phase, I2 can support commander and staff decision making by answering priority intelligence requirements and providing intelligence to support kinetic and non-kinetic targeting. The use of I2 enables targeting in future large-scale ground combat operations by increasing commanders' situational understanding/situational awareness and helping to prevent peer/near-peer threats from gaining positions of advantage.[2]

The exponential growth of foreign data as countries step up surveillance efforts within their borders could prove a boon to the United States and allies in answering commanders' priority intelligence requirements. However, adversaries, unconstrained by U.S. privacy and civil liberties laws, will take full advantage of U.S. persons' publicly available information and seek ways to seize non-public I2 data to answer their own intelligence requirements.

Biometric Data

Biometric data include metrics relating to human features—such as fingerprints, iris scans, facial photos, and voice prints—that could be used to distinguish individuals. Biographical data include name, address, gender, marital status, and birthdate. Behavioral attributes identify people by the ways in which they interact with the world or a device. Examples include how individuals perform the following: walk, known as gait recognition; hold and interact with a device; operate a computer mouse; or type on a keyboard.

U.S. Privacy and Civil Liberties Laws

U.S. agencies engaged in domestic security investigations operate under, and are restricted by, clear legal frameworks pertaining to collecting publicly available information. These include, but are not limited to, Executive Order 12333, the Foreign Intelligence Surveillance Act, Department of Defense (DoD) Manual 5240.01 and various other DoD instructions, and AR 381-10 (*U.S. Army Intelligence Activities*). These legal frameworks ensure that the intelligence community collects, retains, or disseminates information concerning U.S. persons only in accordance with procedures established by the head of the intelligence community element concerned or by the head of a department containing such element and approved by the Attorney General after consultation with the Director of National Intelligence. Collection following these legal frameworks respects U.S. citizens' privacy rights and civil liberties.

Old Idea, New Tools

The idea of gathering large amounts of seemingly innocuous data tied to an identity is not a new concept. As a marketing tool, such efforts have distilled general and individual consumer tastes and preferences for decades. What is rapidly changing is where and how the gathering of artificial intelligence-enabled biometric data is occurring in a world that is increasingly harnessing big data. Also changing is how those data are aggregated with biographical data to become a powerful I2 tool for operational use. Devices such as smartphones have enabled tremendous new and expanded data mining opportunities, even in the most remote villages of the world. Although smartphones provide convenience and services to users, they also serve as tracking devices for marketing firms that can use Global Positioning System location technology to profitably trace users' locations and behaviors for their public and private clients.[3]

Although a privacy-conscious smartphone user in some countries may be able to somewhat minimize his digital footprint, a growing Internet of Things ecosystem has multiplied the sensors that can be used to generate I2 data whether or not users opt in. For instance, many foreign governments are implementing smart cities that enable technology to improve a city's governance, planning, management, and liveability through the gathering of real-world, real-time data from a variety of collection devices. Smart cities are enabled by our digitized world, in which increasingly powerful computer technology, fifth-generation cellular communications, artificial intelligence-enhanced facial-recognition cameras, and inexpensive internet-connected sensors of all kinds are linked. According to one smart city vendor website, by the end of 2020, trillions of gigabytes of data will be generated daily.[4] These data are touted as having the ability to provide insights to help local governments predict where, when, and how city assets (for example, transportation, power generation, and mobility) behave and thereby enable cities to plan for growth, maintenance, and infrastructure development. Smart cities also emphasize public safety—they are increasingly implementing the wide-scale use of artificial intelligence-enabled facial-recognition cameras and vehicle license plate readers to identify law offenders and persons of interest in real time.[5]

Illustration public domain courtesy of Piqsels.com

Cities around the world are rolling out systems designed to gather and analyze data for the public good.

Such smart city efficiency improvements have provided foreign countries with new capabilities to build surveillance systems into their deepest infrastructures, enabling them to use device and social media data to provide citizens with or deny citizens of state-sanctioned benefits. China, for example, mandates that citizens use government-sanctioned mobile phone applications to show their "social credit scores" to vendors and government officials when seeking services. Russia attempts to alter the behavior of certain domestic and foreign audiences through targeted social media influence campaigns.[6] Increasing computational power, in conjunction with the expanding efficiencies of artificial intelligence, enables the fusion and machine-driven analysis of diverse data sources.

Imagine a world in which aggregated I2 databases exist to fuse one's biographical, behavioral, and biometric data (for example, identified images of one's face from official documents, one's voice prints from their phone, social media activities, travel patterns, and even a quantified signature of one's way of walking as seen from public cameras) to locate, identify, and characterize individuals at the whim of governments. This pervasive I2 could be realized in a not too distant future in foreign countries that have the resources and the desire. China has used these tools very effectively to target and forcibly intern whole populations of ethnic minorities in the formerly restive state of Xinjiang.[7]

COVID-19 Outcomes: Privacy Concerns versus Public Health Justifications

Although the COVID-19 pandemic is an epidemiological threat, it serves as a new and powerful driver to increase the depth and scope of these surveillance systems to identify, assess, and track individuals and larger human patterns. Because of COVID-19 and increasing global health concerns, foreign governments in crisis are attempting to use every physical and digital means available to identify and perform contact tracing of infected individuals. Countries such as Singapore, China, Taiwan, and South Korea are attempting to control the epidemic by using mass surveillance of mobile phones, credit cards, rail, and flight data and by using closed-circuit television camera footage to track those afflicted with the virus, ultimately to prevent them from coming into contact with healthy populations.[8] More generally, public health officials are also using this technology to observe, by monitoring overall population movements and travel patterns, whether populations are adhering to social distancing guidelines to slow the spread of the pandemic.[9] For example, one analytic suite of tools, which Italy implemented into one of its smart cities for urban planning, displays anonymized and aggregated location data from connected vehicles' sensors, navigation systems, mobile phone applications, and governmental agency data. At the regional, provincial, and municipal levels, the software generates the daily percentage variation in the number and

Photo illustration by the National Ground Intelligence Center

In the future, smartphones, smart city camera systems, social media, and contact tracing will work together to make surveillance increasingly effective in public areas.

distance of trips compared with January 2020 (the COVID-19 outbreak onset) and the proportion of incoming and outgoing daily and weekly trips according to origin or destination.[10]

Foreign governments that have not previously purchased smart city surveillance systems are very likely seeing the advantages of those systems because of the crisis.[11] Chinese companies, which lead this market, will likely take advantage of the current climate to aggressively market their surveillance systems to previously uninterested or unconvinced customers, or to augment and expand existing installed systems.[12] China has successfully employed facial-recognition technology to control the activity of its citizens within its own smart cities, and now in response to the pandemic, its major technology companies are expanding their mass digital surveillance networks to include people's health data.[13] Vendors will argue that smart city technologies provide the intelligence-gathering and analysis tools critically needed to manage people in urban areas facing COVID-19 and future pandemics. Governments with weak democratic institutions that buy in, armed with emergency powers and increased financial resources to tackle the crisis, will have little incentive to restrict these systems once this particular crisis is over—especially in a world that has been traumatized and now fears the next pandemic.

Disclosed Information	Germany	Hong Kong	New York	Singapore	South Korea	U.K.
Age and gender	*	*	*	*	*	
Geographical breakdown of patients	*	*	*			
Home address (area)		*		*	*	
How case confirmed					*	
Identified contact persons		*			*	
Links to previous cases	*	*		*		
Nationality if case is imported				*	*	
Prior places visited				*	*	
Travel history		*	*	*	*	*
Treatment location		*		*	*	*
Workplace address				*	*	

Table by author, Ms. Christine Kaiser

Personal data governments have released about COVID-19 patients.

Although many foreign countries that have historically protected personal privacy are doing their best to anonymize and compartmentalize the COVID-19 contact tracing information for health professionals only, in other countries, significant I2 data are readily accessible by nonmedical government personnel and thus enable data sharing for agile government responses.[14] Other types of biometric and biographical data, taken from mobile devices, are available for purchase by savvy buyers, including foreign governments using emergency powers (regardless of legalities).[15] Governments will almost certainly also purchase sophisticated and available tools to gain sharper insights from these I2 data to target, trace, and isolate individuals and those with whom they have come in contact.[16]

Looking Ahead: Growing Capabilities and Novel Uses

Massive amounts of I2 data are being generated globally, and the COVID-19 pandemic is loosening restrictions in many foreign countries, enabling the aggregation of data and overlooking the legal frameworks meant to protect privacy. A more sympathetic legal framework driven by public health concerns and coupled with the availability of aggregation tools, training, and maintenance (such as those that smart cities offer) will enhance public sector I2 in the future. Even though privacy concerns limit the collection, usage, and dissemination of data in Western democracies such as the United States, the overall global collection and aggregation of these data are unlikely to cease with the de-escalation of COVID-19 concerns once governments realize how powerful state-level I2 tools are to gain knowledge and insight for managing and potentially even avoiding state-level crises.

From a military perspective, the same technology tools offering the ability to track human patterns broadly or individuals more specifically for epidemiological control could also determine the military-related indications and warnings of adversarial action. As data explodes and governments increasingly harness I2 capabilities to aggregate and make sense of human activity, these digital footprints become an attractive target for adversarial states. The ability to remotely collect identity information—including biographical, biometric, behavioral, and relevant publicly available data about an individual through digital means—can provide the ability to target key players during the competition phase. Competitive defense organizations with these I2 tools, in a digital age, could monitor troop movements, identify and follow message traffic between troops and their families, and analyze foreign military actions and patterns. Those who can obtain, through whatever means, global I2 data troves that countries are increasingly building will have powerfully enhanced abilities to understand who the enemy are, where they are, and what they are planning well before the eruption of open conflict.

During the competition phase of multi-domain operations, the deep fight can be taken to the stateside homeland, where our data are locally generated but become borderless in the cloud because of the internet. In today's digital realm, everyone is connected to the internet to shop, bank, socialize, and work, often using mobile phones that signal exact locations and patterns and that are linked to identities. An adversary that could access these digital footprints could recognize Army reservists getting ready to leave their homes for deployment, conducting revealing travel patterns that serve as indicators. Once deployed, Soldiers will not take their mobile phone with them to observation posts or on patrol; however, as off-duty Soldiers access and post to social media to stay in touch with family, plenty of I2 data valuable to an adversary will continue to be generated. Foreign governments conducting surveillance, data collection, and I2 analysis, initially in response to COVID-19, may have new clarity within their borders to identify patterns of interest from a military intelligence perspective (for example, activity of Soldiers and/or assets in country).

Key Takeaways

In the near future, joint operating environment priorities will potentially undergo shifts due to deployments in regions with highly sophisticated personally identifying data collection, aggregation, and pattern analysis capabilities. These places may have newly enhanced abilities to understand who we are, where we are, and what we are planning, thus posing a threat to cover and to conventional military operations.[17] The I2 data and analysis will help reveal unexpected patterns of movement and behavioral anomalies at individual or group levels that may have been the most effective way to conceal activity previously. In addition, the potential availability of such data in the cyber domain may enable intelligence organizations—both friend and foe—to better understand the operational environment.

Military intelligence officers and military decision makers need to recognize the rapidly developing permissive collection environment that the COVID-19 pandemic has accelerated. This new reality is driving nations to use I2 technology to access and consolidate individuals' data into huge repositories for identity analysis. These new I2 capabilities have implications for the DoD because I2 can be used to inform policy and strategy development, conduct operational planning and assessments, and target individual identities at the point of encounter. Under this new environment, operational decision makers should reevaluate how the U.S. military conducts planning, training, and collection long before the opening of hostilities.

Epigraph

Headquarters, Department of the Army G-2, *Identity Intelligence Concept of Operation* (Draft) (Washington, DC, 2020).

Endnotes

1. Peter Baber, Pamela Baker, and Mark Dotson, "Identity Intelligence Contributes to Multi-Domain Operations," *Military Intelligence Professional Bulletin* 46, no. 1 (January–March 2020): 24–28.

2. Headquarters, Department of the Army G-2, *Identity Intelligence Concept of Operation.*

3. Matthew Johnston, "Smartphones Are Changing Advertising & Marketing," Investopedia, March 26, 2020, https://www.investopedia.com/articles/personal-finance/062315/how-smartphones-are-changing-advertising-marketing.asp.

4. "Build on data for smart cities: What is a smart city?" Autodesk, accessed April 21, 2020, https://www.autodesk.com/solutions/architecture-engineering-construction/smart-cities.

5. Kashyap Vyas, "In What Ways Data Collection in Smart Cities Is Threatening?" Interesting Engineering, January 28, 2019, https://interestingengineering.com/in-what-ways-data-collection-in-smart-cities-is-threatening.

6. Stephan De Spiegeleire, Matthijs Maas, and Tim Sweijs, *Artificial Intelligence and the Future of Defense* (The Hague: The Hague Centre for Strategic Studies, 1 January 2017), https://www.hcss.nl/sites/default/files/files/reports/Artificial Intelligence and the Future of Defense.pdf.

7. Chris Buckley and Paul Mozur, "How China Uses High-Tech Surveillance to Subdue Minorities," *New York Times,* May 22, 2019, https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html.

8. Nicholas Wright, "Coronavirus and the Future of Surveillance," *Foreign Affairs,* April 6, 2020, https://www.foreignaffairs.com/articles/2020-04-06/coronavirus-and-future-surveillance; Shirin Ghaffary, "What the US can learn from other countries using phones to track Covid-19," Vox, April 22, 2020, https://www.vox.com/recode/2020/4/18/21224178/covid-19-tech-tracking-phones-china-singapore-taiwan-korea-google-apple-contact-tracing-digital; and Veronica Combs, "How smart city tech is being used to control the coronavirus outbreak," TechRepublic, March 30, 2020, https://www.techrepublic.com/article/how-smart-city-tech-is-being-used-to-control-the-coronavirus-outbreak/.

9. Yasheng Huang, Meicen Sun, and Yuze SuiHuang, "How Digital Contact Tracing Slowed Covid-19 in East Asia," Harvard Business Review, April 15, 2020, https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia; and Isobel Asher Hamilton, "Compulsory selfies and contact-tracing: Authorities everywhere are using smartphones to track the coronavirus, and it's part of a massive increase in global surveillance," Business Insider, April 14, 2020, https://www.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3.

10. Sue Weekes, “Analytics tool launched to track mobility flows across Italy,” Smart Cities World, 14 April 2020, https://www.smartcitiesworld.net/news/analytics-tool-launched-to-track-mobility-flows-across-italy-5194.

11. Simon Chandler, “How Smart Cities Are Protecting Against Coronavirus But Threatening Privacy,” Forbes, April 13, 2020, https://www.forbes.com/sites/simonchandler/2020/04/13/how-smart-cities-are-protecting-against-coronavirus-but-threatening-privacy/#2088e6a41cc3.

12. Naomi Xu Elegant and Clay Chandler, “When red is unlucky: What we can learn from China’s color-coded apps for tracking the coronavirus outbreak,” *Fortune,* April 20, 2020, https://fortune.com/2020/04/20/china-coronavirus-tracking-apps-color-codes-covid-19-alibaba-tencent-baidu/; and Combs, “How smart city tech is being used.”

13. Ghaffary, “What the US can learn.”

14. Wright, “Coronavirus and the Future of Surveillance.”

15. Chandler, “How Smart Cities Are Protecting.”

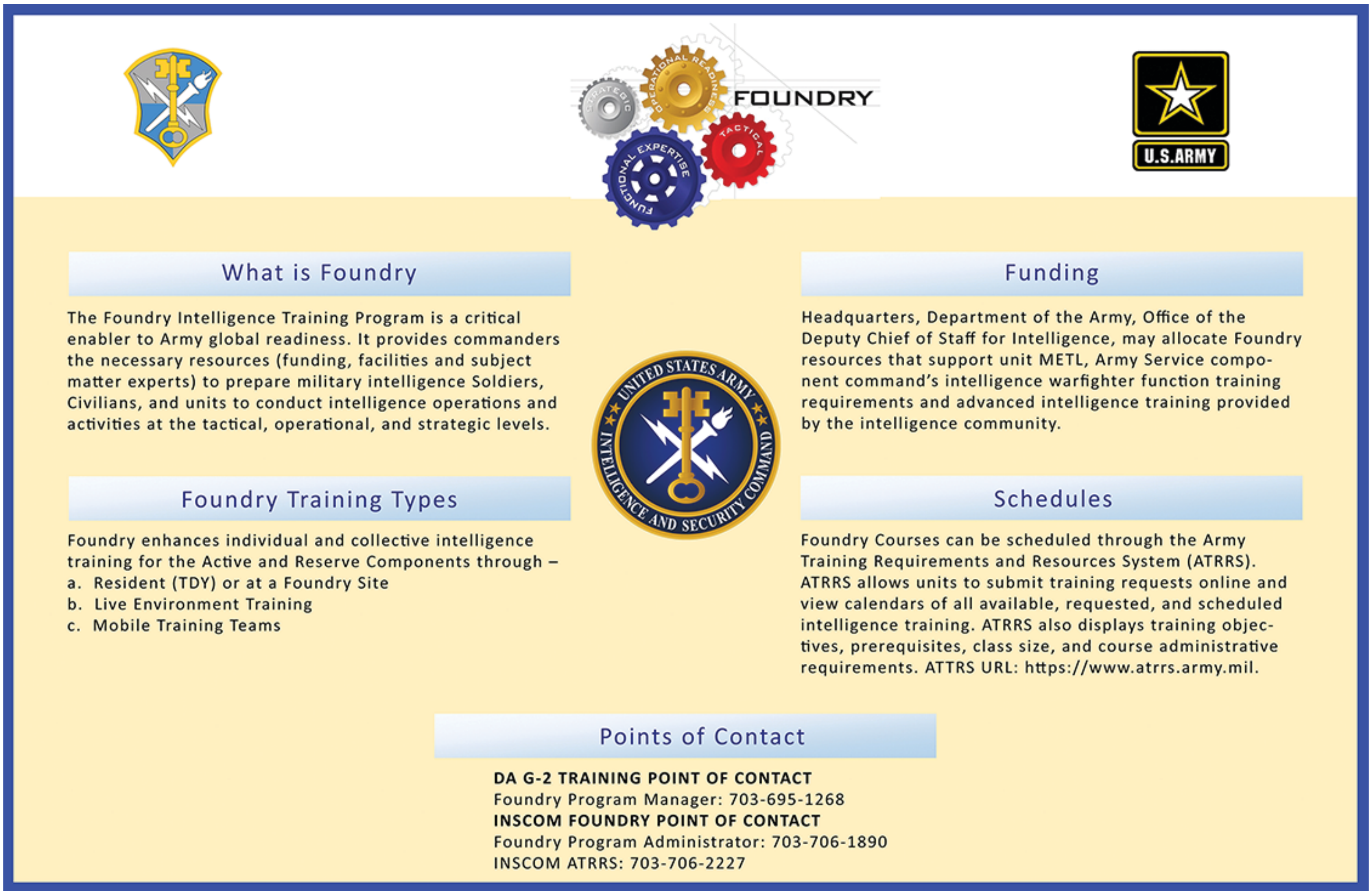
16. Ibid.

17. Der Spiegeleire, Maas, and Sweijs, *Artificial Intelligence*.

Ms. Christine Kaiser serves as an intelligence specialist in the Identity Intelligence Division with the Department of Defense (DoD). She has 20 years of experience as an all-source intelligence analyst, contract analyst, and Army Civilian intelligence specialist; 13 of those years are within the identity intelligence enterprise. She holds a bachelor of science in criminal justice and homeland security.

Mr. Gregory Smith is an analyst for identity intelligence with the DoD. He previously worked with the Federal Bureau of Investigation as an analyst on the National Name Check and Domain Intelligence programs. He holds a bachelor’s degree in foreign affairs from the University of Virginia and a master of science from Colorado State University.

Mr. Kasey Diedrich serves in the Identity Intelligence Division with the DoD. He has 8 years of analysis and production experience, specifically within the identity intelligence enterprise.


STRATEGIC
OPERATIONAL READINESS
TACTICAL
FUNCTIONAL EXPERTISE
FOUNDRY
U.S.ARMY
UNITED STATES ARMY
INTELLIGENCE AND SECURITY COMMAND

What is Foundry

The Foundry Intelligence Training Program is a critical enabler to Army global readiness. It provides commanders the necessary resources (funding, facilities and subject matter experts) to prepare military intelligence Soldiers, Civilians, and units to conduct intelligence operations and activities at the tactical, operational, and strategic levels.

Foundry Training Types

Foundry enhances individual and collective intelligence training for the Active and Reserve Components through –

a. Resident (TDY) or at a Foundry Site
b. Live Environment Training
c. Mobile Training Teams

Funding

Headquarters, Department of the Army, Office of the Deputy Chief of Staff for Intelligence, may allocate Foundry resources that support unit METL, Army Service component command’s intelligence warfighter function training requirements and advanced intelligence training provided by the intelligence community.

Schedules

Foundry Courses can be scheduled through the Army Training Requirements and Resources System (ATRRS). ATRRS allows units to submit training requests online and view calendars of all available, requested, and scheduled intelligence training. ATRRS also displays training objectives, prerequisites, class size, and course administrative requirements. ATTRS URL: https://www.atrrs.army.mil.

Points of Contact

DA G-2 TRAINING POINT OF CONTACT
Foundry Program Manager: 703-695-1268
INSCOM FOUNDRY POINT OF CONTACT
Foundry Program Administrator: 703-706-1890
INSCOM ATRRS: 703-706-2227