Past, Present, and Future Irregular Warfare Challenges: Private Sector Perspectives

Statement of Mr. Mark L. Cohn
Vice President, Engineering and Chief Technology Officer
Unisys Federal Systems, Unisys Corporation

Before the
House Armed Services Committee
Subcommittee on Intelligence,
Emerging Threats and Capabilities

June 28, 2013

Good morning Chairman Thornberry, Ranking Member Langevin, and other distinguished Members of the Subcommittee. I am Mark Cohn, Vice President Engineering and Chief Technology Officer for Federal Systems at Unisys Corporation. We thank you for inviting Unisys to participate in this hearing focusing on lessons learned in irregular warfare, challenges that remain in today's operating environments, and how industry can contribute to enhancing our security.

Unisys is a global corporation, headquartered in Blue Bell, Pennsylvania with 22,000 employees in over 100 countries providing information systems solutions and services to a wide range of private and public sector customers. Unisys has a long and proud history of serving our federal government. We provide solutions for 1500 government entities around the world.

Around the world and here at home, Unisys is a leading provider of integrated security solutions – many of which incorporate advanced biometric and identity management technologies. For example, we delivered a national identification card for Malaysia that employs fingerprint identification and supports real-time biometric verification of identity at traffic stops and biometrically-protected automated border control. We delivered a national identification system for Angola with multiple biometrics that required mobile enrollment in the villages under austere conditions. It provides counterfeit-resistant proof of identity to a large and widely dispersed population, as a cornerstone of citizenship in an emerging democracy to support proof of the right to vote and for future access to multiple government services. Recently, we delivered a system for Mexico that provides for storage of 110 million identification records comprising fingerprints, facial images, and iris scans with the capacity to process 250,000 new enrollments daily. Enrollments are underway starting with youth and extending to Mexico's entire adult population. Mexico's Secretary of Government (SEGOB) stated that the use of iris recognition, along with other biometric data, serves to combat crime such as human trafficking and to streamline registration and enrollment procedures in schools and health care programs. These systems, along with those we furnish to national security and law enforcement organizations, provide reliable technology to verify the identities of known individuals and the means to identify unknown individuals.

To defend the nation and defeat our adversaries engaged in irregular warfare, the Department of Defense requires capabilities in counterterrorism, counterinsurgency, foreign internal defense, and stability operations. Our military operates with other U.S. governmental agencies, multinational partners, and the partner nation to develop plans for coordinated action and to minimize the reliance on U.S. military and security presence. In the long run, it is ultimately a political contest for legitimacy and influence over a relevant portion of the population that depends on a capable local partner to address the conflict's causes and provide security, good governance, and economic development. However, counterinsurgency operations depend on separating enemy combatants from innocent civilians in the general population.

Generally state and/or non-state actors resort to irregular warfare when traditional methods of warfare are not ideally suited to reach their objectives or they do not have the resources to fight against a stronger adversary. In irregular warfare, a primary U.S. objective is to create a safe, secure environment for friendly populations and friendly military forces and to mitigate disruptions to their daily lives. This can help to grow or maintain popular support for the government or entity the U.S. is supporting. Providing a safe environment is complex during irregular warfare as the "enemy" generally is well concealed within the population. The "enemy" can involve a number of non-state actors, such as terrorists, criminal enterprises and warlord militias, that are difficult to identify among the general population, and this enhances their ability to carry out surprise attacks on the population. Another challenge in irregular warfare is being able to distinguish loyal indigenous security forces from disloyal foes who can procure uniforms and equipment that allow them to blend with regular forces and conduct surprise attacks on installations or within government buildings that could have strategic policy implications.

Biometrics, the application of technology and science to measure physical characteristics to determine the identity of individuals, can play a valuable role in irregular warfare by helping to prevent and disrupt irregular threats by identifying targets of interest, deny movement to adversaries, and protect civilians and military forces. It is important to recognize there are limitations to biometric systems and methods as data captured for these purposes by U.S. personnel generally requires close physical proximity to the subject, usually is episodic and selective because cooperative participation by subjects cannot be expected, and relies upon equipment and a system architecture that reportedly fails at times to fully address operational needs. Today's tactical collection equipment employs custom-built integrated mobile kits that can be bulky and cumbersome and reportedly there are issues with data synchronization and other factors limiting effective tactical use (referring to GAO report GAO-12-442, pages 16-24). Industry can help by taking advantage of new mobile processing platforms derived from consumer mobile devices configured for rugged conditions and extended with biometric sensors and by implementing interfaces in a unified architecture that streamlines information interchange from tactical collection to an authoritative database so that submissions are received and match/no-match results are provided to operators consistently and quickly. It is essential that transmitted and stored identity information and biometrics stay coupled because separation of the data undermines the system's speed, accuracy and ability to detect enemy combatants. With respect to facility security and force protection, more advanced biometric techniques than are in use today are possible to improve verification of identity for U.S. and coalition military personnel and civilian partners and without requiring the person undergoing verification close proximity to friendly forces. One example is three-dimensional facial recognition which does not depend on the use of visible light so it can operate at night without calling attention to itself. At facilities and checkpoints, this would allow greater stand-off distances reducing the threats posed by suicide bombers. Another example is improved 2-dimensional and what is called "2.5 dimensional" facial recognition algorithm performance, intelligent camera systems, and face detection analytics that could enable capture of unobtrusive non-cooperative biometric data to identify and associate individuals observed at improvised explosive device detection sites.

Unisys longstanding experience providing integrated biometric credentialing solutions in countries such as Malaysia, Australia, Canada, South Africa, Chile, Costa Rica and Spain indicates that other countries are using wide-scale identity management and biometrics to protect borders, secure transportation facilities, and to improve the efficiency of the administration for public services. Some focus on electoral participation or on delivery of social services. The relative cost and performance of such systems has improved dramatically in the last twelve to fifteen years with greater reliance today on multiple biometrics simultaneously captured for enrollment (not just two fingerprints for example but capturing all ten and adding facial and/or iris), proven large scale adoption of commercial frameworks that reduce development time and risk, and emergence of standards and services based architectures that enable vendor independence in selecting algorithms and building systems that can evolve. The biometric systems that Unisys deployed in Angola and Mexico can be seen as examples where these trends have come together. Both were implemented rapidly at predictable cost because we used a framework of proven components to enable the various delivered systems to be flexible, scalable, secure, and to utilize multiple workflows and biometric modalities independent of the algorithm vendors, and to rely on standards-compliant open interfaces.

There has been a great expansion in the number of economically viable use cases for biometrics to support access control such as neighborhood policing (badging systems for use at checkpoints to achieve local area security), protecting access to government buildings and military installations, humanitarian assistance identification systems to reduce fraud in distribution of aid, and international border control systems to improve security. For instance, we implemented a system that the Port of Halifax that uses vascular biometrics for access to the port by 5,000 workers and the Restricted Area Identity Card with fingerprint and iris for access to Canada's 28 major airports. DNA matching is now more widely used in forensic identification systems to combat crime and also increasingly for purposes such as kinship analysis for disaster victim identification. In all regions of the world, we see widespread user acceptance of biometrics for secure access to sensitive facilities including international borders and for consumer convenience such as protecting electronic banking records and securing air travel. Consumer mobile applications will increasingly rely on biometrics captured with inexpensive sensors (for voice, face, and touch). There is significant commercial interest in banking and other regulated industries because anti-spoofing techniques can easily be employed and biometrics can simplify the user experience while increasing security when compared with password or personal identification number (PIN). This could provide advantages for some purposes over today's Department of Defense personnel authentication approach that relies on Common Access Card (CAC) and PIN. A commercially available biometrics-driven alternative used today in the banking sector would be more convenient, less expensive and time consuming to administer, would eliminate the problem of transport and lockout during PIN reset, and could address risks such as the impostor threat that the current CAC and PIN model cannot. Low cost and deployment "footprint" mean this could be used to secure access by non-government organizations and partner country personnel to electronic systems for sharing situational awareness information.

We believe the Department of Defense can expect that these international and industry developments are in many cases applicable to the challenges we face when confronting adversaries in irregular warfare and in improving the internal security and stability of the societies that we are working to stabilize both through U.S. and partner country initiatives. Unisys looks forward to supporting that progress both here and overseas.