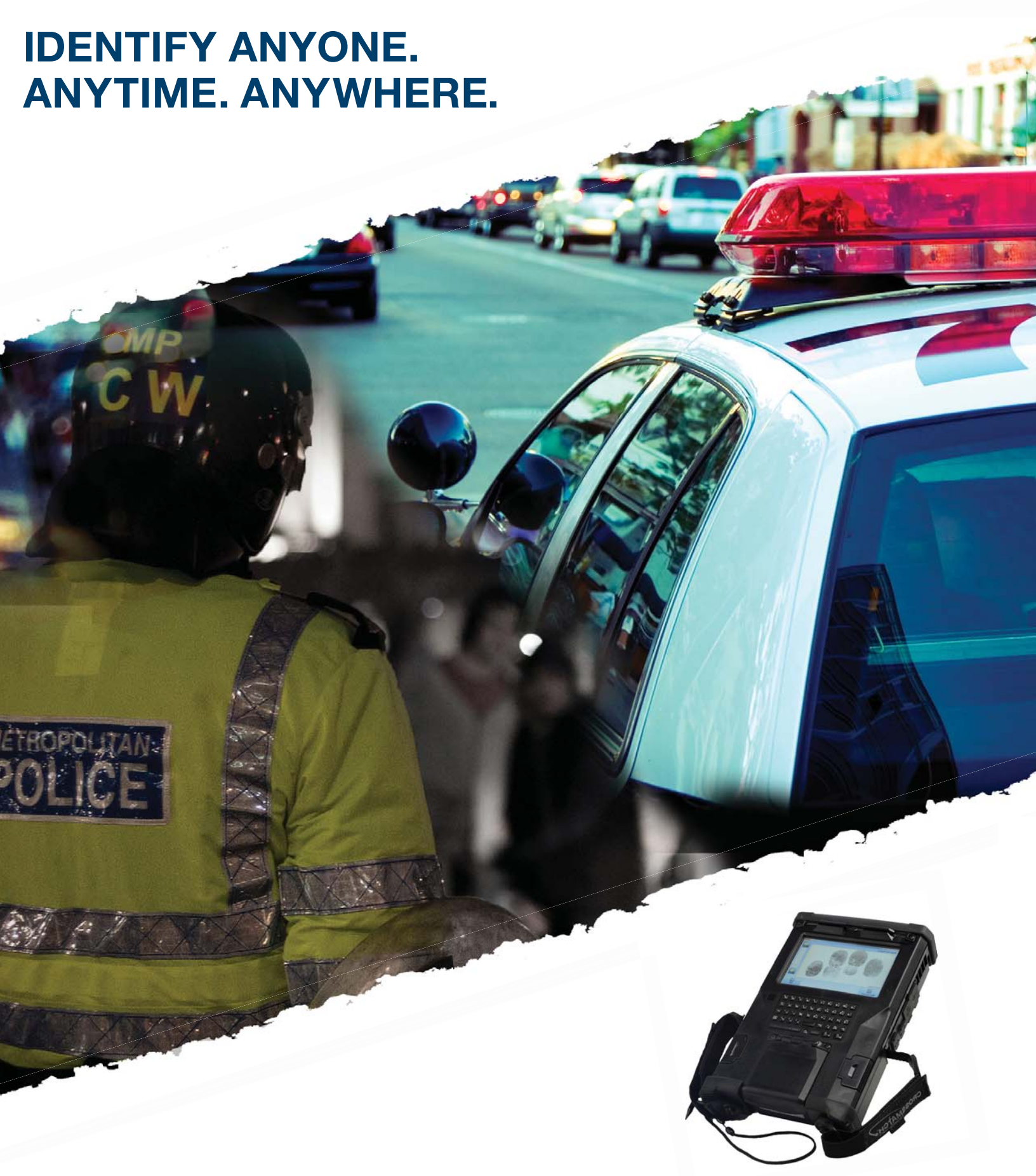
Biometrics and National Security White Paper

This white paper provides a cursory overview of the biometric security initiatives that the U.S. military engages in within theaters of war.

Rawlson O`Neil King
Lead Researcher, Biometrics Research Group, Inc.

IDENTIFY ANYONE.
ANYTIME. ANYWHERE.



SEEK® Avenger

The benchmark for rapid mobile multi-biometric identification, enrollment, and credential reading. Purpose-built to perform in the harsh and challenging environments of the military, border security, and law enforcement professional.

Get all the facts at www.crossmatch.com/seek-avenger.php

CROSSMATCH® TECHNOLOGIES

TABLE OF CONTENTS

Research Methodology

Biometrics Research Group, Inc. uses a combination of primary and secondary research methodologies to compile the necessary information for its research projections.

The conclusions drawn are based on our best judgment of exhibited trends, the expected direction the industry may follow, and consideration of a host of industry drivers, restraints, and challenges that represent the possibility for such trends to occur over a specific time frame. All supporting analyses and data are provided to the best of ability.

Primary Research

Biometrics Research Group, Inc. conducts interviews with technology providers, clients, and other organizations, as well as stakeholders in each of the technology segments, standards organizations, privacy commissions, and other influential agencies. To provide balance to these interviews, industry thought leaders who track the implementation of the biometric technologies are also interviewed to get their perspective on the issues of market acceptance and future direction of the industry.

Biometrics Research Group, Inc. also applies its own proprietary micro- and macroeconomic modeling using a regression analysis methodology to determine the size of biometric and related-industry marketplaces. Using databases of both publicly and privately-available financial data, Biometrics Research Group works to project market size and market potential, in the context of the global economic marketplace, using proven econometric models.

Secondary Research

Biometrics Research Group, Inc. also draws upon secondary research which includes published sources such as those from government bodies, think tanks, industry associations, internet sources, and Biometrics Research Group, Inc.'s own repository of news items. This information was used to enrich and externalize the primary data. Data sources are cited where applicable.

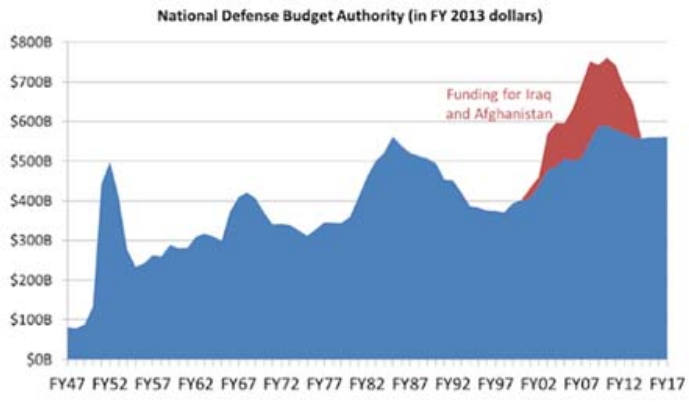
National Security: An Introduction

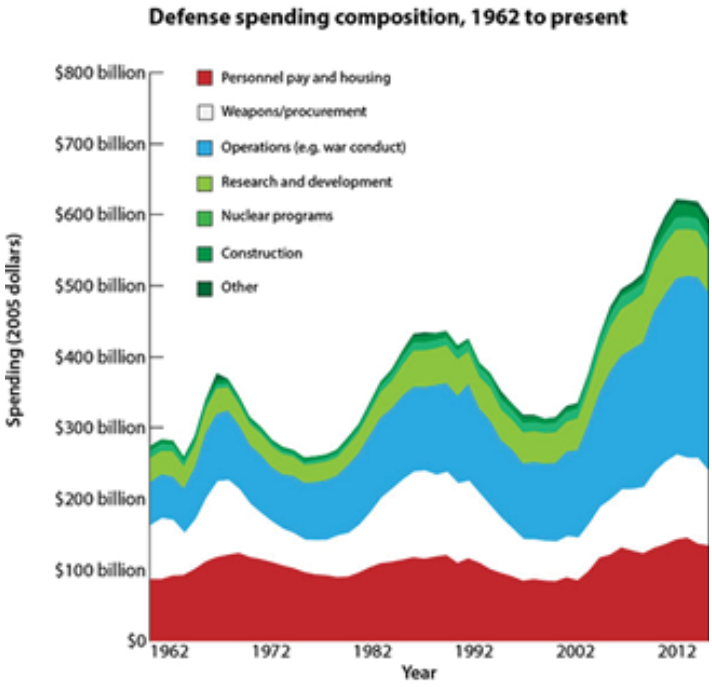
Biometrics Research Group, Inc. defines "national security" as the requirement to maintain the survival of the state mainly through the use of power projection. This involves maintaining effective armed forces; ensuring the resilience and redundancy of critical infrastructure; using intelligence services to detect and defeat or avoid threats and espionage, protecting classified information; and using counterintelligence to protect a nation from internal threats.

U.S. Military Budget Projections

In terms of spending, the Biometrics Research Group estimates that the United States spends more than US$1.2 trillion per annum on national security. This spending includes the costs in aggregate for the Global War on Terror, homeland security, spending on the U.S. intelligence community, veteran's affairs, pensions and associated debt servicing costs.

In focused terms, the 2014 federal budget provides US$526.6 billion specifically for the Department of Defense's base funding in 2014, representing a decrease of $3.9 billion, or 0.7 percent, below the 2012 enacted level.





This level of funding arguably provides sufficient resources to carry out the national U.S. defense strategy, while drawing down the U.S. military presence in Afghanistan. The 2014 federal budget also arguably provides sufficient funds for research and development efforts.

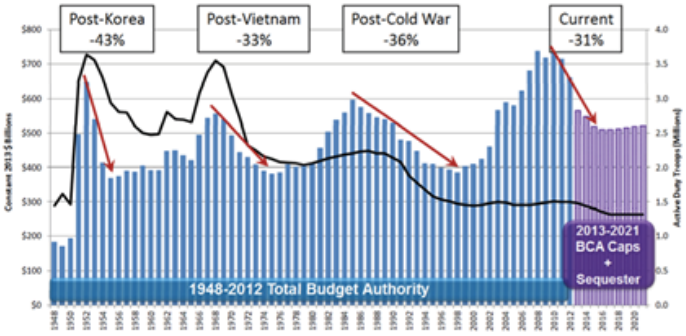
The 2014 budget will provide US$67.5 billion for defense research, development, test and evaluation activities.

In specific terms, the budget will include US$12 billion for early-stage science and technology programs. This funding supports basic research, applied research and advanced technology development. The budget also provides US$2.9 billion for the Defense Advanced Research Projects Agency (DARPA) and its breakthrough research, an increase of 1.8 percent above the 2012 enacted level.

Biometrics Research Group now estimates that total U.S. Government spending is at least US$700 million per annum on basic biometric research. Much of this research is undertaken within the national security framework and will continue to be funded at healthy levels, despite severe spending cuts caused by budget sequestration.

While the U.S. Government will still allocate a tremendous amount of its spending authority on national security, the sequestration process, which implements a mandatory austere fiscal policy, will affect discretionary defense spending. The impasse over sequester between the executive and legislative branch began in March 2013, and as a result of previous fiscal negotiations, will slowdown government spending.

Over the 2014–2023 period, if sequester continues unabated, planned spending outlays will be reduced by US$995 billion, with interest savings of $228 billion, for a total of over US$1.2 trillion in debt reduction.



The Congressional Budget Office projected in February 2013 that under the "sequester" and Budget Control Act caps:

- Defense spending outlays (including "overseas contingency operations" for Iraq and Afghanistan) will be reduced from US$670.3 billion in 2012 to approximately US$627.6 billion in 2013, a decrease of $42.7 billion or 6.4 percent. Defense spending will fall again to US$593.4 billion in 2014, a decrease of US$34.2 billion or 5.5 percent.

- Defense spending will rise gradually from US$593 billion in 2014 to US$714 billion by 2023, an annual growth rate of 2.1 percent during the 2014 to 2023 period and 0.6 percent for the 2012-2023 period. The 2.1 percent growth rate approximates CBO's projected rate of inflation and is well below the annual spending growth rate of 7.1 percent from 2000-2012.

- Defense spending will fall steadily from 4.3 percent GDP in 2012 to 2.8 percent GDP by 2023. Defense spending averaged 4.0 percent GDP from 1990 to 2012, ranging from 3.0 percent GDP to 5.2 percent GDP.

Due to the projected decline in defense spending, Biometrics Research Group expects a slight reduction in U.S. government spending on biometrics. Some of the reduction in spending will be directly attributable to the completion of military action in Afghanistan. The U.S. military had been actively engaged in using biometrics in the battlefield. The end of the active military operations will cause a reduction in acquisition of biometric equipment for deployment in the field.

Because of the highly competitive nature of nation states and the fluid state of the world order, national security preparedness depends as much on routine technical measures and operational procedures as on central decision making. This ranges from information protection to state secrets to weaponry to the use of high-end technologies such as biometrics.

U.S. Military Biometric Program Guidance

Biometrics Research Group defines biometrics as measurable physical and behavioral characteristics that enable the establishment and verification of an individual's identity. Biometric patterns can be anything from fingerprints, iris scans, facial recognition or even voice recognition.

Several U.S. Department of Defense organizations are involved in developing guidance on the collection and use of biometrics data. The Secretary of Defense designated the Secretary of the Army as the Executive Agent for Defense Biometrics. Subsequently, the Secretary of the Army designated the Director of the Army's Biometrics Task Force as the Executive Manager for Biometrics, making her responsible for developing guidance for collecting and processing biometrics data. Additionally, DOD appointed the Director, Defense Research and Engineering, as the Principal Staff Assistant for Biometrics. The Director has developed and issued a biometrics directive identifying organizational

roles and authorities for managing biometrics data.

Biometrics data -- and the sharing of these data among federal agencies -- is important to the United States' broader national security mission beyond DOD's operations in Afghanistan and Iraq. Homeland Security Presidential Directive 6, issued in September 2003, states that it is the policy of the United States to develop, integrate, and maintain terrorist information, and to use that terrorist information as appropriate and to the full extent permitted by law to support certain screening and other processes, including military, intelligence, law enforcement, immigration, and visa processes. In accordance with this and other laws and regulations, DOD, the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and the Department of State (DOS) share biometrics information.

The Intelligence Reform and Terrorism Prevention Act created an Information Sharing Environment, defined as an approach that facilitates the sharing of terrorism and homeland security information, with a Program Manager responsible for information sharing across the federal government. Additionally, the National Science and Technology Council, part of the Executive Office of the President, has created a subcommittee to address the use of biometrics across the federal government.

Within DOD, the Deputy Secretary of Defense, in a January 2007 memorandum, stated that DOD would immediately adopt the practice of sharing unclassified DOD biometrics data with other U.S. departments and agencies with counterterrorism missions. According to the memorandum, this includes data related to terrorism information defined in the Intelligence Reform and Terrorism Prevention Act regarding terrorists, detainees, and those individuals or groups posing a threat to the United States, U.S. persons, or U.S. interests, but excludes data pertaining to U.S. persons, defined as U.S. citizens and aliens lawfully admitted for permanent residence. Non-U.S. persons are individuals who are neither U.S. citizens nor aliens lawfully admitted into the United States for permanent residence.

The memorandum further states that sharing unclassified biometrics data unrelated to terrorism information will be determined based upon relevant law and directives but will require, at a minimum, a written memorandum from a requesting agency stating the official need for the data, the intended use of the data, the protections and safeguards that will be afforded the data, and the nature or extent of possible further distribution of the data to other organizations or agencies.

Further, the memorandum stated that sharing of biometrics data on an individual must be conducted pursuant to U.S. law and regulations and international agreements where appropriate.

The U.S. government currently does not maintain a comprehensive, government-wide, biometrics-based terrorist database or watch list. In the absence of such a database or watch list and to increase the utility of the biometrics data it collects, DOD has established relationships—both with its own components and with interagency and multinational partners—through which it can share standardized biometrics files, analyses, and associated information in order to match results and determine whether there is a link between an individual's biometrics file and available associated information.

Gaps in DOD's and other agencies' biometrics collection and sharing processes can increase the risk that terrorists will avoid identification in subsequent encounters with U.S. personnel during military operations, the visa application process, and U.S. border crossings. For example, during the visa application process or at a U.S. entry point, if terrorists are not identified as such, U.S. personnel may unknowingly grant them access to the United States. While a number of biometrics databases exist across the federal government, there are three

major federal biometrics databases that include, among other data sets, information on known and suspected terrorists: (1) the FBI's Integrated Automated Fingerprint Identification System (IAFIS); (2) DOD's Automated Biometric Identification System (ABIS), which is collocated with IAFIS; and (3) the DHS Automated Biometric Identification System (IDENT), which is used by DHS for border patrol, customs, naturalization, and counterterrorism activities, as well as by DOS as part of its visa approval process.

DOD, the FBI, DHS, and DOS have established formal and informal arrangements, pursuant to applicable U.S. laws and regulations and international agreements, regarding the sharing of information among the IAFIS, ABIS, and IDENT databases. The U.S. Department of Defense regards biometrics as a key capability that can identify enemies and deny the anonymity necessary to hide and strike at will. The ability to identify and verify individuals is also regarded as critical to ensure secure and expeditious other key business functions. The military intends to integrate and apply biometric capabilities through various tactics, techniques and processes, to enable a wide range of possible missions, from military operations to business functions that protect national interests.

The Department of Defense coordinates its biometric efforts through its Biometrics Identity Management Agency. The agency acts as the lead military proponent for biometrics, and heads the development of biometric technologies for combatant commands, services and agencies. Its primary goal is to empower war fighters through improving operational effectiveness on the battlefield. The Biometrics Identity Management Agency leads defense activities to program and synchronize biometrics concepts, technologies and capabilities.

Biometric Collection Processes in Theaters of War

During DOD field activities, such as those in Afghanistan and Iraq, U.S. forces collect biometrics data for a variety of purposes, such as to control access to U.S. bases in order to protect personnel and to identify and verify non-U.S. persons that they encounter. The primary system for biometrics data collection in U.S. Central Command, including Afghanistan and Iraq, is the Biometric Automated Toolset. The Biometric Automated Toolset is a DOD biometrics system that allows U.S. forces to collect fingerprints, iris scans, facial photographs, and biographical information of persons of interest and store them in a searchable database.

DOD has also established the Biometric Identification System for Access, which includes similar types of biometrics data but is limited to use on installations in Iraq to determine whether non-U.S. persons should have access to U.S. bases.

Once U.S. forces have collected the biometrics data, they attempt to compare and match the data to previously collected data stored in the Biometric Automated Toolset and the Biometric Identification System for Access. These data are also sent to Automated Biometrics Identification System (ABIS), the department's authoritative, multimodal

biometric data repository—the DOD-wide database for non-U.S. persons' biometrics operated by Biometrics Identity Management Agency—to determine if U.S. forces have previously encountered an individual and entered the individual's biometrics data into this database. If there is not a match, the new data are stored in the Biometric Automated Toolset and ABIS and maintained for future use, as appropriate.

ABIS enables military agencies to conduct automated fingerprint searches, store images electronically, and exchange fingerprints on an on-demand basis. The system incorporates fingerprint, mug shots and DNA collection. In Iraq and Afghanistan, ABIS has also been utilized to help counter the problem of improvised explosive devices (IEDs), tracing fingerprints back to those who make and detonate IEDs.

The Biometric Automated Toolset contract was awarded by the U.S. Army to GTSI, a provider of technology solutions to federal, state, and local governments.

The contract, awarded in August 2011, was for mobile biometric devices that would assist soldiers in real-time identification of persons of interest in the field. The contract had a total value of $159 million. The award covered a 16-month period and was executed as part of GTSI's Information Technology Enterprise Solutions 2 Hardware (ITES-2H) contract with the federal government.

GTSI partnered with Cross Match Technologies, Inc., a leading manufacturer of biometric solutions, to deliver a portable solution that provides a rugged platform capable of capturing multiple biometric modalities in the field.

BAT includes an enrollment kit consisting of a laptop and attached biometric collection devices capable of enrollment, verification, and identity detection, together with mobile handheld devices for collecting, storing, and uploading pertinent data to U.S. Army biometrics collection centers. A system of servers containing the biometric database maintains and synchronizes information, ensuring that data collected at one location is available at others. Description of U.S. Military Use of Biometric Technologies in the Field

U.S. forces currently collect biometrics data on non-U.S. persons in Afghanistan at roadside checkpoints, base entry control points, and during patrols and other missions. The U.S. military is engaged in utilizing biometric data to enhance their operational capability on the battlefield. U.S. forces use three principal biometrics collection devices to enroll individuals:

Biometrics Automated Toolset: The toolset consists of a laptop computer and separate peripherals for collecting fingerprints, scanning irises, and taking photographs. The Toolset system connects into any of the approximately 150 computer servers geographically distributed across Afghanistan that store biometrics data. The Toolset system is used to identify and track persons of interest and to document and store information, such as interrogation reports, about those persons. This device is primarily used by the Army and Marine Corps to enroll and identify persons of interest.

Handheld Interagency Identity Detection Equipment: Is a self-contained handheld biometrics collection device with an integrated fingerprint collection surface, iris scanner, and camera. The Handheld Interagency Identity Detection Equipment connects to the Biometrics Automated Toolset system to upload and download biometrics data and watch lists. This device is primarily used by the Army and Marine Corps.

Secure Electronic Enrollment Kit: Is a self-contained handheld biometrics collection device with a built-in fingerprint collection surface, iris scanner, and camera. Additionally, the Secure Electronic Enrollment Kit has a built-in keyboard to facilitate entering biographical and other information

about individuals being enrolled. The Kit is used primarily by the Special Operations Command, although the Army and Marine Corps have selected the Kit as the replacement biometrics collection device for the Handheld Interagency Identity Detection Equipment.

U.S. forces in Afghanistan collect biometrics data and search for a match against the Afghanistan biometrically enabled watch list that is stored on the biometrics collection devices in order to identify persons of interest. Soldiers and Marines connect their biometrics collection devices to the Afghanistan Biometrics Automated Toolset system's architecture, at which point the data are transmitted and replicated through a series of computer servers in Afghanistan to a database in West Virginia. Special operations forces have a classified and an unclassified Web-based portal that they use to transmit biometrics data directly from their collection devices to the database in West Virginia.

Biometrics data obtained during the enrollment using the biometrics collection devices are searched against previously collected biometrics records in the Afghanistan biometrically enabled watch list, and in some cases the Biometrics Automated Toolset servers, before searching against stored biometrics records and latent fingerprints stored in the database. Match/no match watch list results are reported to Task Force Biometrics and other relevant parties. The biometrics data collected during the enrollment are retained in database for future matching by defense agencies.

Once collected, biometrics data and associated information are evaluated by intelligence analysts to link a person with other people, events, and information. This biometrics-enabled intelligence is then used to identify persons of interest, which can result in his or her inclusion on the biometrically enabled watch list. The biometrically enabled watch list for Afghanistan contains five levels, and according to the level of assignment, an individual who is encountered after his or her initial enrollment will be detained, questioned, denied access to U.S. military bases, disqualified from training or employment, or tracked to determine his or her activities and associations.

In addition to DOD, the Federal Bureau of Investigation and the Department of Homeland Security collect and store biometrics data to identify persons of interest. The Federal Bureau of Investigation uses its biometrics system for law enforcement purposes. The Department of Homeland Security uses its biometrics system for border security, naturalization, and counterterrorism purposes, as well as for visa approval in conjunction with the Department of State. While the three biometrics organizations are able to share information, the biometrics databases operate independently from one another.

U.S. Military Personnel Training on the Use of Biometrics

The Army, Marine Corps, and Special Operations Command have trained thousands of personnel on the use of biometrics prior to their deployment to Afghanistan over the last eight years. This training includes the following:

• Army: Offers classroom training at its three combat training centers at Fort Polk, Louisiana; Fort Irwin, California; and Hohenfels, Germany as well as home station training teams and mobile training teams that are available to travel and train throughout the United States as needed. In addition, the Army is developing virtual-based training software to supplement its classroom training efforts.

• Marine Corps: Offers classroom training at its training centers at Camp Pendleton, California and Camp LeJeune, North Carolina as well as simulation training at Twentynine Palms, California.

• Special Operations Command: Offers classroom and simulation training at Fort Bragg, North Carolina. Moreover, the military services and Special

Operations Command have mobile training teams in Afghanistan to provide biometrics training to personnel during their deployment. Additionally, the military services rely on personnel who have been trained in biometrics prior to deployment to train others while deployed.

The Office of the Secretary of Defense, the military services, and Central Command each has emphasized in key documents the importance of training.

The 2008 DOD directive, which was issued by the Under Secretary of Defense for Acquisition, Technology, and Logistics, four years after biometrics collection began in Afghanistan, emphasizes the importance of biometrics training, including the need for component-level guidance to ensure training is developed as required. The Office of the Assistant Secretary of Defense for Research and Engineering subsequently drafted an implementing instruction that includes guidance for the establishment of training programs designed to enable DOD units and leaders to effectively employ biometrics collection capabilities and utilize biometrically enabled watch lists. Both the Army and Central Command have issued guidance that requires soldiers to be trained prior to deployment.

Additionally, an Army regulation on training says that first and foremost, training must establish tasks, conditions, and standards to prepare units to perform their missions. Similarly, a Marine Corps order on training states that units focus their training effort on those missions and tasks to which they can reasonably expect to be assigned in combat. This Office of the Secretary of Defense, Army, Marine Corps, and Central Command guidance underscores the importance of biometrics training.

BiometricUpdate.com reported in June 2013 that the 17th Infantry Brigade, which is part of the First Army Division, undertook a weeklong biometrics training program. The program was intended to help integrate biometric technologies into the mobilization program of the U.S. Army.

The brigade engaged in a 40-hour training program focused primarily on how to operate biometric equipment. Soldiers were taught how to correctly enroll and identify individuals, along with the proper management of their data files. A team comprised of military and civilian experts taught the course.

Scope of Biometric Equipment Usage & Equipment Upgrades

Since 2004, U.S. forces in Afghanistan have collected biometrics from more than 1.2 million individuals with approximately 3,000 successful matches to enemy combatants. The fielding of newer military grade biometrics equipment is also currently occurring in Afghanistan. Forward operation personnel have seen their old handheld Interagency Detection Equipment replaced with the Secure Electronic Enrollment Kits, developed by Cross Match Technologies.

Combining forensic-quality fingerprint capture, rapid dual iris scan capability and innovative facial capture technology, the kit, entitled SEEK II, is a comprehensive, multimodal identification and enrollment platform. The compact, portable solution is designed for rugged field use, making it quick and easy for military, border control and U.S. government agencies to identify subjects and verify their identities in the field.

The platform automatically captures and formats standards-based flat and rolled fingerprints, iris and facial images, which conform to the Electronic Biometric Transmission Specification (EBTS). This Department of Defense specification describes customizations of FBI Electronic Fingerprint Transmission Specification (EFTS) transactions, which are necessary to utilize AFIS databases, including the DoD ABIS. Using SEEK II, military forward operations can create fingerprint, iris and facial-based biometric records for enrollment into the military ABIS system.

A versatile system, SEEK II leverages a 120,000-person watch list, which can easily be updated to match the current "known and suspected terrorists" (KST) list, for biometric data comparison. This capability is extremely valuable to field personnel in remote locations for performing on-the-spot ID checks. The built-in wireless networking capability allows field personnel to access remote databases, such as ABIS, for thorough identification checks. Additionally, SEEK II can be configured to capture and hold latent images in a database for remote matching.

The kit does not only enroll an individual but also launches a simultaneous search to determine if a person is on a watch list.

Soldiers at the ground level are expected to collect not only usable biometric data but also enroll civilians who are willing to submit themselves. According to the U.S. military, over 19,000 persons in Afghanistan have been enrolled using the SEEK II kit. Out of this number enrolled with the SEEK II, the U.S. Marine Corps notes that approximately 300 have been placed on a watch list. The Marines have revealed in the last year, that more than 2,000 Marines and coalition troops have received training with the device and that at least 15,000 units have reportedly been shipped to military personnel around the world.

On the software backend, the Department of Defense has contracted with Science Applications International Corporation (SAIC) to provide software engineering maintenance and management services in support of the U.S. military's tactical biometric collection capability.

SAIC will work with the military to capture biometric data and enroll it into the Department of Defense's (DoD) enterprise authoritative biometric database. The aim is to aid in positively identifying and verifying the identity of actual or potential adversaries. The contract, worth US$73 million, was awarded to SAIC under the U.S. Army's Computer Hardware, Enterprise Software and Solutions (CHESS) Information Technology Enterprise Solutions 2 Services (ITES-2S) contract vehicle. Work will be primarily performed in Alexandria, Va., Williamsburg, Va., Charleston, S.C., Sierra Vista, Ariz., and Fairmont, W.Va.

Conclusions

The importance of biometric technology in military operations has grown significantly since the events of September 11, 2001. In addition to the conventional capability of verifying a claimed identity for access control purposes, biometric technologies have the unique capability of verifying that an individual is not a member of a particular group of interest (e.g., terrorist or enemy combatant).

Biometric technology also facilitates positive identification, i.e. identifying who an individual actually is as opposed to who the individual claims to be. The goal of creating an identity dominance capability, where U.S. forces have the distinct ability to separate "friend or foe," is paramount to any military conflict that involves asymmetrical warfare.

Enemies to the United States have employed sophisticated methods to exploit flaws in identity management systems in order to carry out terrorist attacks in the past, and the U.S. military has committed to blunt and eventually eliminate this capability.

As a consequence, the U.S. military has acknowledged that the need for technologies that can provide for better border security, force protection, and counterterrorism measures has never been greater.

The effectiveness of this ability to identify adversaries will ultimately depend upon collection and maintenance of data in interoperable formats that can be shared among U.S. Government organiza-

tions, as well as with partner governments through appropriate agreements, when the need arises. Biometric data collected from persons of interest will continue to include physical characteristics and traits that can be used to identify an individual included any identification system. To ensure this data is accessible and usable to the fullest extent possible, the systems that utilize biometric data will leverage appropriate standards wherever possible.

Military commanders note that the ultimate goal of "tactical systems" is to provide operational assistance to soldiers in battlefield situations. The military believes that biometrics is an important tool well suited to this task. Biometrics will therefore continue to be a key technology for deployed personnel engaged in terrain operations, despite any defense budget restraint.

About the Biometrics Research Group, Inc.

Biometrics Research Group, Inc. provides proprietary research, consumer and business data, custom consulting, and industry intelligence to help companies make informed business decisions.

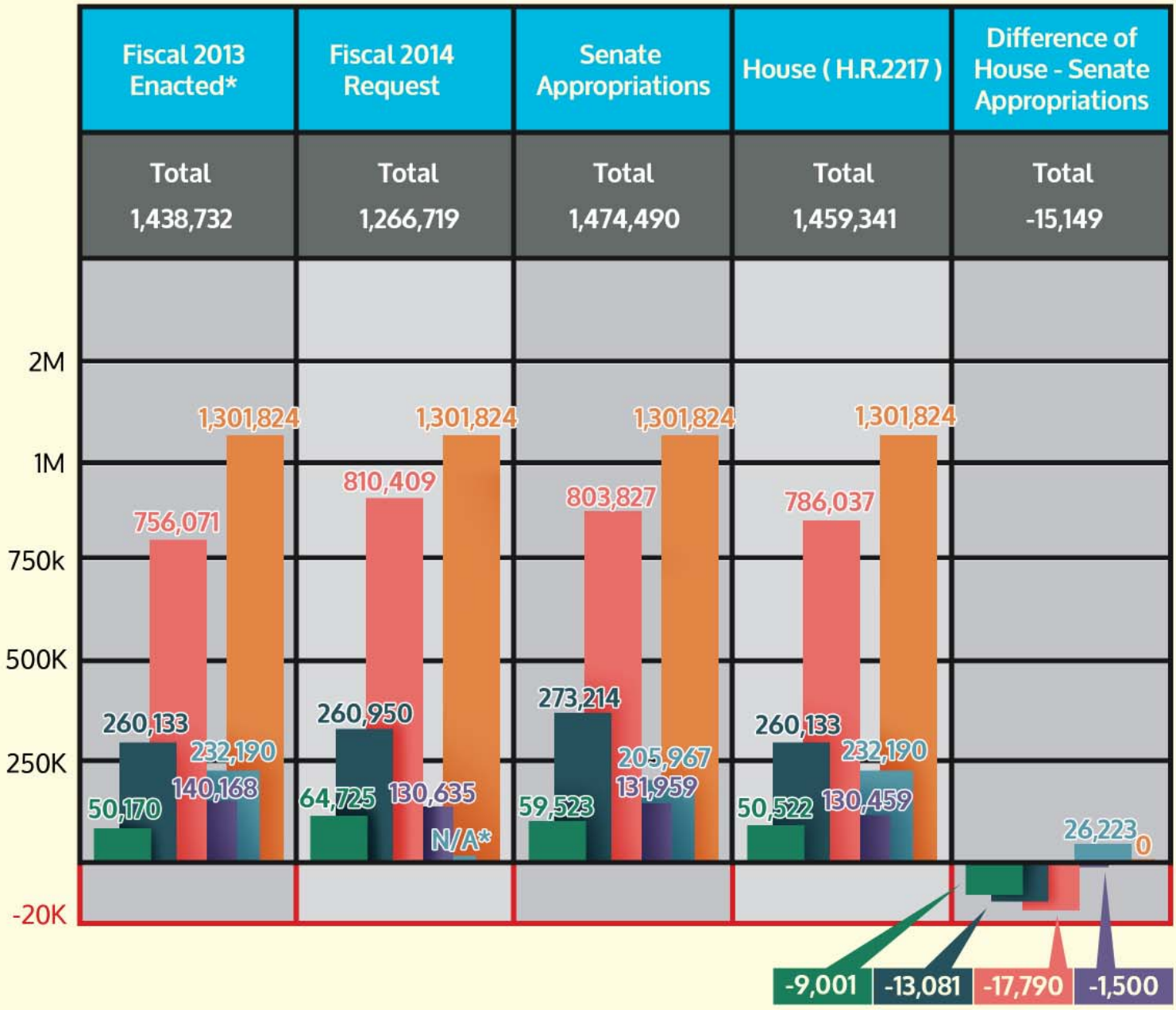
We provide news, research and analysis to companies ranging from Fortune 500 to small start-ups through market reports, primary studies, consumer research, custom research, consultation, workshops, executive conferences and our free daily BiometricUpdate.com news service.

Biometrics Research Group has positioned itself as the world's preferred supplier of pure-play market research and consultancy services focused on the biometric marketplace, which particular focus on the law enforcement and national security sectors. Our portfolio of white papers and full research reports is based upon high-quality quantitative analysis, allowing our clients to gain deeper understanding of the marketplace.

We customize our research design, data collection, and statistical reporting using proprietary micro- and macroeconomic modeling and regression analysis.

Through integration of our research results with qualitative analysis from our BiometricUpdate.com news service, we provide actionable business analysis.

NPPD FISCAL 2014 APPROPRIATIONS (NUMBERS = THOUSANDS)



*Where the House and Senate differ due to inclusion of recessions, we,ve gone with the House figure.
**This is a US-VISIT account realigned into NPPD by the second fiscal 2013 continuing resolution (P.L. 113-6). *Source: House and Senate committee reports. Image: FierceHomeland Security*