BIOMETRICS TASK FORCE

ANNUAL REPORT FY07

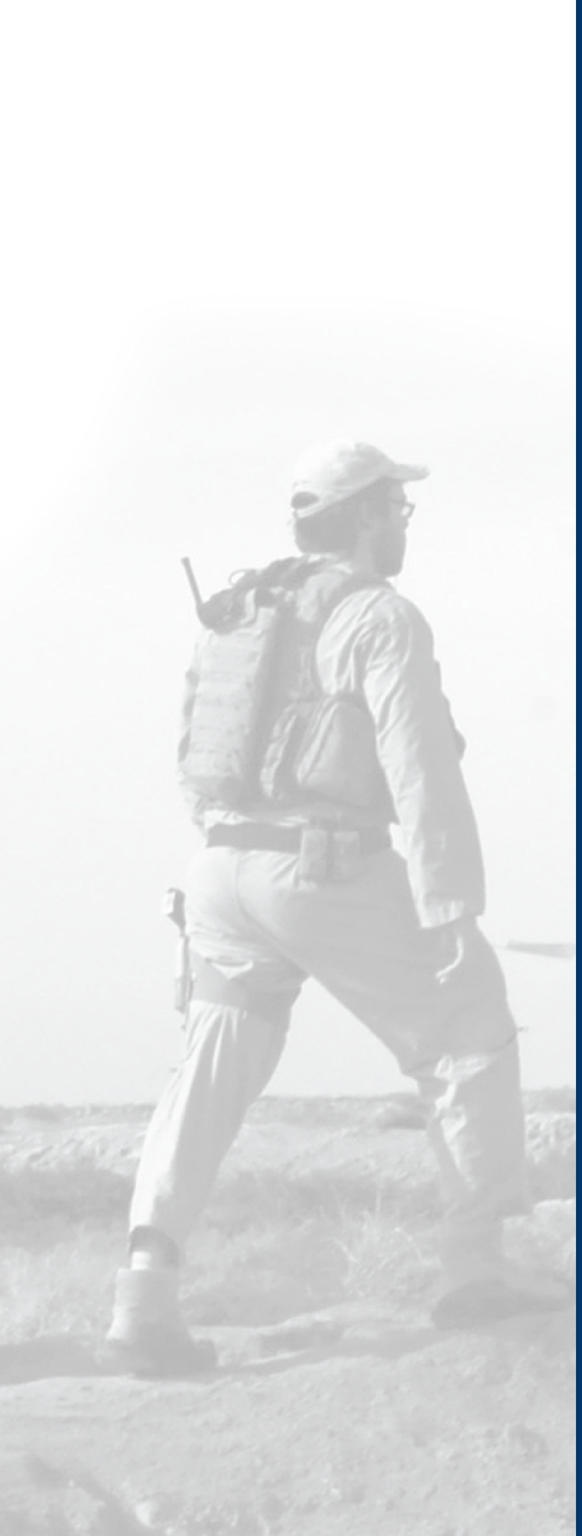
“Distribution Authorized to U.S. Government Agencies and their contractors only to protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary. Information of this type may be classified or unclassified; when unclassified, it is export-controlled and subject to the provisions of DoD Directive 5230.25 (reference (c)). (1 Oct. 2007). Other requests for this document shall be referred to DAMO-SPT-BIO.”

http://www.biometrics.dod.mil

BIOMETRICS

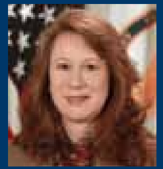
TASK FORCE

ANNUAL REPORT FY07



2007

REPORT FROM THE DIRECTOR



DR. MYRA GRAY

As we look back on 2007, we see significant movement and growth in the application of biometric technologies in the Department of Defense (DoD) mission, both for access and to help identify known threats within the theater of active operations in Iraq and Afghanistan. We are proud to be helping develop and field those technologies that help protect the lives of Warfighters in theater and at home. As we progress through FY08, the Biometrics Task Force (BTF) is poised to ramp up to a new stage of growth.

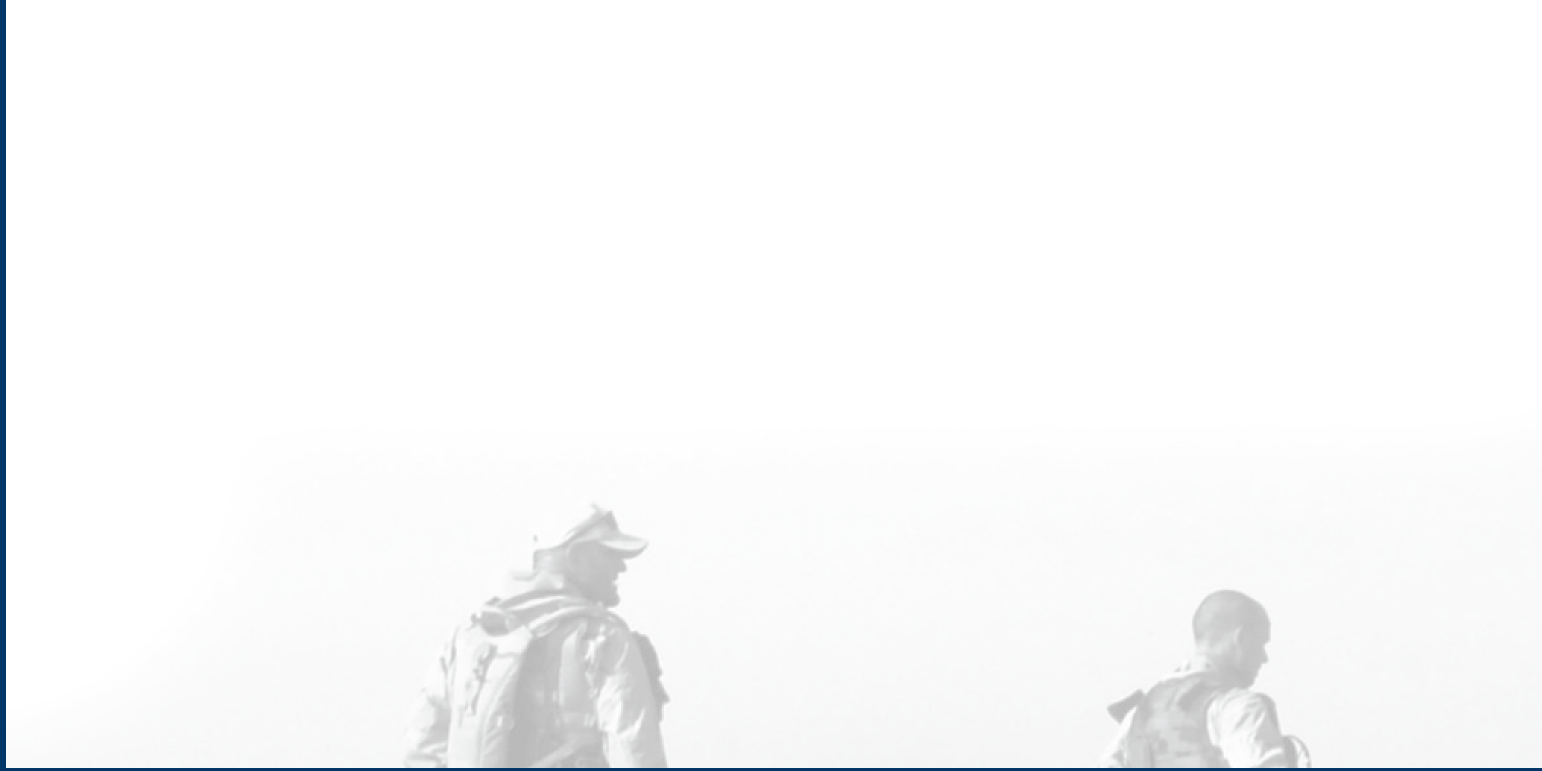
While I write this, we expect that the Table of Distribution & Allowances will be approved shortly. With this formal declaration, the BTF will have permanent staffing — including representatives from multiple organizations within the DoD — and, with our partners in Project Manager (PM) DoD Biometrics, will develop an efficient and effective way ahead for applications throughout the Department.

This annual report provides an overview of our 2007 initiatives, highlights financial data about the BTF program, and demonstrates the impact of our work.

I invite all members of the biometrics community throughout DoD, other executive agencies, and industry to take part in our efforts. We are here to work with you to ensure that the best technologies are made available to our troops.

Very Respectfully,

Dr. Myra Gray

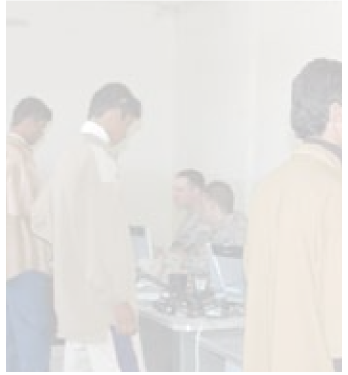


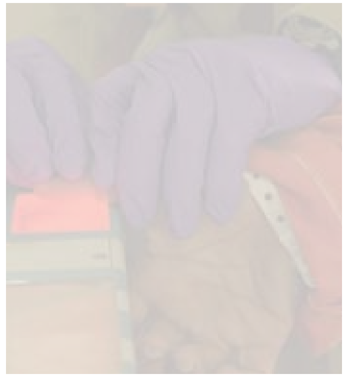
CONTRIBUTIONS

PART 1

ORGANIZATION AND MISSION

This section includes summary information about the mission and organization of the BTF.

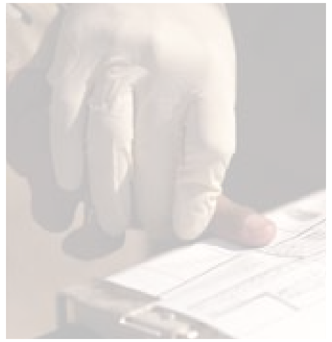




WHAT ARE BIOMETRICS?

Biometrics are measurable, physiological, and/or behavioral characteristics (fingerprints, iris, DNA, voice, facial features, etc.) that are distinct and can be used to verify the identity of an individual. Biometrics can tie an individual to past acts and aliases or can be used to permit access to facilities and data.

Typically biometrics are used to answer either:
"Are you who you claim to be?" (verification); or
"Have we encountered you before?" (identification).



ORGANIZATIONAL OVERVIEW

The Biometrics Task Force leads Department of Defense (DoD) activities to program, integrate, and synchronize biometric technologies and capabilities and to operate and maintain DoD's authoritative biometric database to support the National Security Stategy. The BTF operates through the Executive Agent authority given to the U.S. Army and delegated to the G-3/5/7. The BTF executes day-to-day biometric functions and leads coordination for strategic movement forward for all parts of the DoD, in cooperation with the Director, Defense Biometrics (DDB) and Project Manager (PM) Biometrics. PM Biometrics, under the authority of the Program Executive Office for Enterprise Information Systems (PEO EIS), has responsibility for acquiring common and joint materiel solutions. The BTF is supported by multi-Service governance structures that capture Service and user requirements, provide coordination of science & technology efforts, and identify and resolve biometrics-related issues. The BTF roles and responsibilities were clarified in a new DoD Directive (DoDD) on Biometrics, currently awaiting formal issuance. Further definition will follow in a DoD Instruction.

Housed primarily in Arlington, Va., and Clarksburg, W.Va., the BTF is composed of the Biometrics Integration Directorate (BID) and the Biometrics Operations Directorate (BOD). The BID is responsible for establishing the strategic direction for biometrics use in DoD, leading the development of biometrics standards, policy, and architecture, and coordinating liaison activities across the Services, other DoD organizations, and other government agencies. The BOD operates the authoritative DoD database for adversary and neutral forces biometrics, tests and evaluates biometric equipment, and supports field operations of the equipment used by the various Services in theater and in the Continental United States (CONUS).

HISTORY OF THE BTF

The DoD began implementing biometric technologies in 2000 following a feasibility study commissioned in 1999 by the U.S. Congress. This study demonstrated that biometric technologies were an emerging capability that would have a significant impact on the DoD and needed to be formalized, centralized and funded. The Biometrics Management Office (BMO) was established within the chain of command of the Army's Chief Information Officer (CIO). The Secretary of the Army was named as Executive Agent (EA) for the DoD, making the BMO the focal point for biometrics for all of the military branches and DoD agencies. The mission at that time focused on Information Assurance (IA), particularly network access.

In the fall of 2000, the Biometrics Fusion Center (BFC) opened in Clarksburg, W.Va. Reporting to the BMO, the BFC was tasked with testing commercial biometric products for accuracy and compatibility with DoD information systems. Over the next three years, the BMO and BFC were heavily involved in running pilot projects to evaluate the practicality of using biometric technologies for managing both network and physical access. Work began on designing the backbone architecture needed to pass biometrics data securely and quickly between DoD installations and vessels. Development of standards for biometric templates, files, software, and hardware began in earnest. The BMO became a significant contributor in the development of DoD, federal, and international standards for biometrics. At the same time, the BMO began to identify and develop formal policies regarding biometrics as the need arose.

After the September 2001 terrorist attacks, the DoD developed a vision for using biometrics to lock down the identity of known or suspected terrorists. This represented an expansion of the BMO and BFC mission beyond simply keeping American facilities and networks secure. To accomplish this, the DoD saw the need for a biometrics collection and storage system compatible with the established Integrated Automated Fingerprint Identification System (IAFIS) used by the Federal Bureau of Investigation (FBI). In 2004, the DoD Automated Biometrics Identification System (ABIS) became operational. This IAFIS-compatible database gave the DoD a centralized storage point for biometric data collected by the military.

As the ABIS developed, biometric systems that had already been in use for verification purposes began adapting so that the data captured by them were compatible with ABIS.

EQUIPPING THE WARFIGHTER

Operations Enduring Freedom and Iraqi Freedom made it clear that Warfighters needed more advanced tools for distinguishing known terrorists and insurgents from friendly populations and that biometric technologies could help fill that need.

Operations Enduring Freedom and Iraqi Freedom made it clear that Warfighters needed more advanced tools for distinguishing known terrorists and insurgents from friendly populations and that biometric technologies could help fill that need.

As the focus of the BMO and BFC swung toward identification of enemy combatants and terrorists, Army and DoD leadership saw that biometric technologies were playing less of an IA-focused role and more of an operational role than originally envisioned. In 2006, this led to moving the BMO and BFC from reporting to the Army CIO (with DoD oversight from the Assistant Secretary of Defense for Networks and Information Integration) reporting to the Army Chief of Operations (G-3/5/7). The Director, Defense Research and Engineering (DDR&E), Office of the Secretary of Defense for Acquisition Technology & Logistics, was named as the Principal Staff Assistant for Defense Biometrics. At that time, the BMO and BFC were reorganized into the Biometrics Task Force (BTF) to better represent its mission to support the Warfighter. The BTF shifted toward testing biometric systems and software that support the capture of biometric data for enrollment in or matching against the ABIS.

The value of the ABIS and various biometric collection and verification platforms has been repeatedly demonstrated since 2004. With data in the ABIS expanding to more than 1.5 million records by summer 2007, biometric matches gave the Warfighter a tool to aid in distinguishing between friend and foe. For example, some Iraqi personnel applying for selection to the Iraqi Police Academy were found to have biometric records as terrorists or insurgents. Some detainees in theater were matched to felony records in the United States. As the collection, transmission, and storage systems have matured, the frequency of such matches has increased. At the same time, the response time to answer "Should I detain or not?" has decreased, helping the Warfighter to protect himself and other Coalition forces by quickly separating suspected enemies from the general population. Although the ABIS can quickly determine if there is a biometric match, it cannot determine the value of that match. Is it a match between the fingerprints of a known terrorist and a police academy applicant or between a previously cleared U.S. facility employee and a police academy applicant? The need for this "so what" information has led to new relationships between DoD law enforcement and the DoD intelligence community. These groups can determine the value of a match and then help get that answer back to the Soldier, Sailor, or Marine who needs to know “Should I detain or not?” Much of the work at the BTF focuses on facilitating the architecture, policy, and relationships that get this information quickly back to the Warfighter.

Biometric technologies other than fingerprint technologies are also in use at the BTF. Prototype iris matching has been performed, resulting in unexpected iris scan matches when there were no previous connections between the individuals using only fingerprint data. When biometric fingerprint records were examined by certified fingerprint examiners, different identities were shown to be the same person. This demonstrates the value of not only iris biometrics, but that of modality fusion as well.

Interagency matches of iris records between FBI and DoD foreign detainee databases have also yielded results. Agreements between the Department of Justice and the DoD have made this type of data sharing possible. The BTF is moving ahead with establishing not only common technical architectures with non-DoD federal agencies, but also the policies to allow sharing of biometric data while ensuring that legal and privacy rules are followed.

The need for biometric technologies in the DoD is clear. As a result, the scope of their deployment will only increase. Along with using biometrics for identifying the enemy, biometrics will soon be used for managing base, building, and network access in accordance with federal guidelines that ensure commonality across the government. Identification of the enemy will also increasingly be a shared governmental function, requiring a common architecture and shared infrastructure across the government. American citizens will not tolerate a situation in which the Department of Homeland Security, after taking biometric data, would grant entry into the United States to a person that the DoD can identify as an enemy based on his or her biometric file. A great amount of work is required to tie together biometric and biographic watch lists and the technical architecture to collect and match biometrics across federal agencies. The BTF is meeting these challenges and giving the DoD the tools to make it happen.

A Table of Distribution and Allowances (TDA) for the BTF is expected to be approved in early 2008, setting a permanent framework that all parts of the DoD community can leverage. Working together, we will implement the biometrics mission across all five Armed Services.

PART 2

FY 07 PERFORMANCE REPORT

This section provides the BTF’s FY07 Performance Report on key measures.

STRATEGY DIVISION

THE STRATEGY DIVISION

The Strategy Division works to establish strategic direction for the DoD Biometrics Program to enable employment of biometric capabilities, including establishing concepts and plans to ensure unity of effort across the biometrics enterprise, coordinating DoD policies to enable joint, interagency and multinational employment of biometric capabilities, and implementing strategic communications that promulgate the DoD Biometrics strategy.

PLANS BRANCH

BACKGROUND

The Plans branch develops the BTF way forward based on national-level guidance and develops and leads implementation of the long-term strategy for realizing the benefits of using biometrics across the DoD. In addition to overseeing the development of strategic plans, the Plans branch supports the development of DoD-level documents and the coordination of plans and timelines in support of stakeholder priorities and overarching enterprise objectives.

ACCOMPLISHMENTS

In FY07, the Plans branch had three major accomplishments:

1. Developed and established the Joint Biometrics Governance Structure and executed the first meeting of the Joint Biometrics Operational Coordination Board (JBOCB) and the Joint Biometrics Senior Executive Steering Committee (JBSESC).

Impact: This provides two centralized forums for the DoD Biometrics community to collaborate and develop solutions to operational issues while concurrently documenting, tracking, and comparing requirements across all DoD components.

2. Published the Capstone Concept of Operations for DoD Biometrics at the beginning of FY07 after four months of intensive writing and staffing.

Impact: This provides the DoD Biometrics community with an enterprise-level description of how to employ and operationalize biometrics. Describes the biometrics process as an enabler to DoD military operations and business functions.

3. Provided support to PSA-led development of DoD Directive 8521.aaE, "DoD Biometrics." The directive completed staffing at the O-6, Flag Officer/General Officer, and OSD levels. As of December 2007, the directive is in final coordination for signature by the Deputy Secretary of Defense.

Impact: The publication of DoDD 8521.aaE "establishes DoD-level policy and assigns responsibilities for the various components within the Department of Defense."

4. Developed the BTF concept plan and draft TDA, providing the framework for a formally-recognized, long-term organization.

Impact: Approval of the TDA will formally recognize BTF's ensuring role and will allow for hiring permanent staff, leading to greater stability of the organization and improved effectiveness.

POLICY BRANCH

BACKGROUND

The BTF Policy branch researches, analyzes, and reviews biometrics and other related DoD policies and drafts and coordinates DoD biometric policies. The Policy branch is responsible for the development of analyses and opinions on the impact of existing or proposed policies on the overall biometrics mission and functions carried out by the BTF. In addition, the branch keeps abreast of legislation that impacts the biometrics program and specific policies in development and maintains archives of such policies and laws for easy reference.

The Policy branch provides the underpinnings for operational and tactical success and is crucial in formulating effective biometrics use strategies across the DoD. Correct policy and legislative interpretations and evaluations allow for strategies to be implemented successfully. In addition, the Policy branch brings the BTF perspective to any new DoD biometrics policies and ensures that the proper equities are reflected in those policies, thus optimizing mission effectiveness.

ACCOMPLISHMENTS

In 2007, the Policy branch contributed to several significant policy objectives. The BTF reviewed and provided textual input to two memoranda from the Deputy Secretary of Defense released in January 2007 addressing sharing of biometric data with interagency and Coalition partners. In addition, the Policy branch has made numerous contributions to the draft DoD Directive (DoDD) on Biometrics and served as the point of contact for all Army inputs to the directive. BTF Policy has also taken the lead in researching, analyzing, and formulating a draft policy decision for sharing biometric equipment and data with the governments of Iraq and Afghanistan, which is expected to be released in 2008.

Impact: The policies regarding the sharing of biometric data have increased the likelihood that terrorists and enemy combatants will be identified and captured before they strike. These policies ensure that organizations such as the FBI and DHS, as well as our Coalition partners, have the ability to screen out likely terrorists while carrying out their routine identification and verification functions. The DoDD will result in greater clarity and division of responsibility for biometric data and equipment within the DoD. This will elevate the biometrics program to a higher level of optimization throughout the Department, as well as the federal government. Policy governing the sharing of biometric data and equipment will likely result in decreased insurgent attacks and an enhanced ability by Iraq and Afghanistan to manage identities within their respective populations, ultimately aiding the political stability of these countries.

FUTURES BRANCH

BACKGROUND

As the use of biometrics has matured within the DoD, requirements identified by Warfighters have increased in complexity. Some requirements are readily met with current equipment and resources found in DoD or industry. However, an increasing number of user demands cannot be addressed with today's technologies and require solutions that have not yet been developed. To address these complex biometric technology requirements, several organizations across the DoD are conducting independent Science and Technology (S&T) efforts. In the past, these S&T efforts have been compartmentalized and uncoordinated across the DoD. To address this issue, the BTF is coordinating DoD S&T plans and developing a DoD S&T roadmap. This will document the current S&T efforts performed across the Department and guide future projects to maximize S&T resources.

ACCOMPLISHMENTS

S&T COORDINATION

In 2007, the Futures branch reached out to entities across the Department to share the biometrics S&T vision and gain insight into the greater DoD S&T process. Meetings were held with representatives from the Assistant Secretary of the Army for Acquisition, Technology, and Logistics, the Army G-3, and the Army G-8.

These discussions identified important information that has been incorporated into the biometrics S&T plan and provided the BTF with a clearer understanding of the S&T process. The BTF participated in two Biometrics S&T workshops sponsored by the Director, Defense Biometrics (DDB) and included representatives from across the Services and agencies within the Department

Impact: The workshops helped to establish an S&T baseline and to begin the process of developing an S&T roadmap for the DoD Biometrics Program.

S&T PLANNING

To understand the current biometrics S&T environment, the Futures branch developed a Biometrics S&T Baseline by collecting data from all parts of the DoD S&T community. The intent for the Baseline was to capture all biometrics S&T projects pursued across the Department. In response to an initial data call, eight offices and 29 funded S&T projects were identified. Using the Biometrics S&T Baseline as a building block, the Futures branch has begun developing a Biometrics S&T Near-Term Plan. This plan maps the current requirements to solutions already pursued within the Department and to S&T projects identified in the baseline. From this analysis, gaps have been identified that will inform the strategy for FY08 S&T funding. The Biometrics S&T Near-Term Plan is currently in draft form and will be completed in early FY08.

Impact: The Biometrics S&T Baseline was shared with others across the DoD S&T community and provided all interested parties with a thorough perspective of biometrics S&T efforts across the Department. This facilitated coordination among researchers and provided senior leaders with a holistic view of current biometrics S&T projects.

CONCEPTS & TECHNOLOGIES BRANCH

BACKGROUND

The Concepts and Technologies (C&T) branch works with government, industry, and academia to explore solutions to requirements and evaluate concepts to enhance the effectiveness of biometrics in DoD. The C&T branch also provides expertise where biometrics and identity technologies may be used within existing DoD processes and mission threads to increase the effectiveness or assurance of those processes. The C&T branch was established in January 2007 to enable a diversely equipped, multi-functional team to address the complex issues associated with concept development and demonstration The branch brought together personnel from several BFC teams, including the Warfighter Support and Software Engineering teams and subject matter experts specializing in various topics, including biometric stand-ards and modalities, electrical and computer engineering, training, project management, graphic design, and others. This diverse group of experts and engineers is uniquely equipped to conceptualize, plan, develop, and demonstrate new capabilities employing biometric devices, systems, and concepts. Within the C&T team, a core group of project managers organizes and coordinates resources to conduct studies, interact with other Services and agencies, conduct experiments and evaluate new concepts and technologies to inform the requirements process.

ACCOMPLISHMENTS

Despite shifting roles and responsibilities during 2007, the C&T branch continued to progress in identifying new opportunities. The C&T branch has been heavily involved in iris experimentation, particularly with the Retica algorithm. During the past year, the Futures branch has developed an iris test image database and an equipment suite to baseline and compare iris algorithms.

Successes include:

- Demonstration of multimodal biometric matching.

  Impact: This effort identified more than 5,000 matches that were not made with the fingerprint modality.

- Establishment of a database platform for multimodal research and engineering.

  Impact: DoD now maintains a secure, controlled repository for multimodal biometric templates and images for use in evaluating concepts and potential solutions.

- Development and deployment of general & pilot system-specific training materials.
- Assistance in technology experimentation events and pilots.
- Provision of subject matter expert support to organizations seeking to learn about, use, or enhance biometric capabilities to support their mission needs.
- Participation in information exchange and collaboration with academia on research and development projects, e.g., meetings of the Center for Identification Technology Research (CITeR) to approve and track progress of projects funded by CITeR.
- Participation in workshops and conferences sponsored by the National Science Foundation (NSF) & National Institute of Standards and Technology (NIST) to discuss the latest technology and research in biometrics.
- Contribution to the Biometrics S&T Roadmap activities by providing technical analysis of data call projects and proposals.
- Participation in the Capabilities Based Analysis for biometrics.
- Contribution to the development of biometric standards.

Impact: These activities helped shape biometric research to enhance capabilities, provided technical expertise for the most effective solutions, and enhanced partnerships with a variety of DoD users.

STRATEGIC COMMUNICATIONS BRANCH

BACKGROUND

The Strategic Communications branch holds a key role in the development of BTF initiatives and the messages shared with the DoD community and the outside world. Strategic Communications works directly with the G-3 Office of the Chief, Public Affairs (OCPA) and BTF leadership to shape an outreach plan, find speaking opportunities, and develop and strengthen relationships with the greater biometrics community. The branch is responsible for overall communications planning, public affairs, conference support, multimedia production, graphics, education, editing, and website construction and management.

AGGRESSIVE SUPPORT

...shaping an outreach plan, finding speaking opportunities, and developing and strengthening relationships with the greater biometrics community.

ACCOMPLISHMENTS

STRATEGIC COMMUNICATIONS PLANNING

The outreach team continued to execute the communications strategy approved in FY06 while developing proposed strategies for 2007 and 2008. Working with the Plans Division of OCPA, the branch determined the way ahead for outreach for the BTF in 2007. Until the BTF transitions to a full TDA organization with an approved name, mission, vision, and organization chart, staffing will be delayed. However, the outreach team continued to work closely with OCPA to respond to reporter inquiries.

Impact: In FY07, these efforts helped to establish the BTF as the focal point for DoD biometrics and to differentiate it from the former Biometrics Management Office.

PUBLIC AFFAIRS

Public Affairs efforts included training, interviews, responses to media inquiries, and writing of articles for military publications. The BTF Director, the acting BTF Deputy Director, and the Director of the BFC all received executive media training.

Impact: This official Army program built confidence in working with the print, radio, and television media as well as helping to consolidate BTF answers for possible media questions.

Articles were written and interview requests were fielded about the BTF for a number of publications, including Military Information Technology Magazine, Fall 2007 issue; Military Intelligence Professional Bulletin; Inside the Army; Congressional Quarterly; and the Frederick (Md.) News-Post.

Impact: Outreach through the media helped publicize the operational capabilities of biometrics in the field.

The BTF Acting Deputy Director was interviewed on National Public Radio (NPR) as a guest on NPR's "Talk of the Nation" program. The host discussed today's employment of biometrics.

Impact: Effectively communicated how the Services are using biometrics in Iraq to separate law-abiding citizens from insurgents.

CONFERENCE SUPPORT

The BTF maintained an aggressive calendar of support to DoD conferences throughout FY07. The BTF outreach team managed all aspects of planning and supporting these events to advocate the BTF mission, impact, and criticality to DoD biometrics efforts. Selection of conferences followed the strategic communications plan focusing on events that reached the Services, the Combatant Commands, government biometrics and identity management organizations, other related government agencies, biometrics academia, and the biometrics industry. The BTF exhibited at the following events in FY07.

2006 Association of the U.S. Army (AUSA) Annual Meeting
Attendees include Army, DoD, U.S. government, industry, and foreign militaries. This is the largest Army meeting and exhibition of the year, drawing between 30,000 and 35,000 attendees.

Armed Forces Communications and Electronics Association (AFCEA) West 2007
AFCEA West, sponsored by AFCEA and the U.S. Naval Institute, focuses on upcoming tactical and materiel revisions in the military and is the largest Navy conference. BTF personnel projected the BTF mission and current efforts supporting Expanded Maritime Interception Operations to more than 5,000 technology professionals from military installations, including Space and Naval Warfare Systems Command (SPAWAR), U.S. Pacific Fleet Command, Naval Base Coronado, Naval Station San Diego, and Marine Corps Camp Pendleton.

2007 Identity Protection and Management (IPM) Conference
The BTF co-hosted the conference with the DoD Public Key Infrastructure Program Management Office (PKI PMO) and the Access Card Office (ACO). The BTF provided subject matter experts to speak on biometrics basics, standards, and watch lists. More than 550 policy makers, program managers, developers, users, and information technology (IT) and physical

security professionals responsible for acquiring, integrating, or supporting identity management technology attended. The BTF and 27 other organizations exhibited at the conference. Participation in this event ensured that BTF efforts in biometrics for physical and logical access are in line with ACO and PKI PMO initiatives.

FiestaCrow Technical Symposium
FiestaCrow is one of the largest USAF-specific symposiums of the year and is a key venue for the BTF to advocate its mission, impact, and criticality to DoD biometric efforts.

2007 GovSec Conference & Exposition
This annual event focuses on the collective needs of federal, state, county, and local homeland security leaders nationwide. This is a key venue for the BTF to advocate its mission, impact, and criticality to the homeland security community. Attendees included government physical and IT security professionals, the U.S. law enforcement community, and first responders from across the country.

2007 U.S. European Command (EUCOM) Technology Expo
This expo, held in Germany, consisted of five shows at four different installations (Stuttgart, Mannheim, Heidelberg, and Grafenwoehr). The BTF provided an exhibit to educate EUCOM personnel on DoD biometrics initiatives and services and on biometrics in general.

2007 Force Protection Equipment Demonstration (FPED) VI
This large biannual event focuses on all aspects of force protection for the DoD, federal agencies, and state and local law enforcement communities. Attendees included members of all of the Armed Services and many federal agencies and law enforcement officials.

2007 Biometric Consortium
The Consortium is the largest government-focused biometrics event of the year. The BTF had support from two personnel from PM Biometrics to augment the booth staff. The outreach team also supported the BTF by coordinating speakers and topics for the plenary sessions. The annual Consortium Conference has the largest gathering of biometric vendors of any event in the United States.

Impact: Participation in these events helps to educate attendees and vendors on DoD biometric initiatives and services and on biometrics in general and promulgates the BTF message to a broad DoD audience. Participation establishes the BTF role within the DoD and facilitates dialogue with vendors, junior and senior enlisted personnel who carry the technology upward, officer-level decision makers who push technology downward, and other government agencies and academia.

MULTIMEDIA SUPPORT

The BTF produced a four-minute operational biometrics video for use at venues throughout DoD. The video production crew interviewed leaders at the BTF and the U.S. Navy and U.S. Marine Corps liaisons on how biometrics affects operations in theater. The outreach team coordinated with assets in Iraq and Afghanistan to shoot fresh footage of biometrics in use in theater.

Impact: The video will promote the use of biometrics and inform viewers of ways in which biometrics are enabling identity superiority in theater.

GRAPHICS SUPPORT

The BTF outreach team developed a new poster campaign for the office. The new poster campaign uses the slogan “Protecting our Greatest Asset” along with images of soldiers in theater using biometric devices. The graphics team also designed a new booth exhibit, logos, coasters, badge lanyard pulls, ABIS brochures, initiatives handouts, pens, and coin designs.

Impact: Graphics help depict the value and relevance of the BTF mission in relation to the Warfighter, BTF members, and other stakeholders in the BTF mission.

EDUCATIONAL PROGRAMS

- Briefed the Joint Biometrics Study Panel on Biometrics 101.

  Impact: Gave panel members from the Naval Research Advisory Committee and the Army Science Board the same baseline knowledge and vocabulary to begin their study.

- Provided Biometrics Technology Training for the Defense Security Service Academy DoD Security Specialist Course.

  Impact: Being a recurring part of this curriculum is a cost-effective way for the BTF to reach a broad, DoD-wide audience focused on security. These students will be responsible for selecting and implementing biometric systems for physical facility security, perimeter security, and information systems security.

- Submitted a scientific paper titled “Fingerprint Image Quality Measurement Algorithm” for publication in the Journal of Forensic Identification (JFI).

  Impact: Publication in this type of peer-reviewed periodical demonstrates that the BTF plays a significant role beyond the operational sphere of biometrics. BTF involvement in the biometrics scientific community is effectively shaping biometric technology development.

- Participated in the Department of Homeland Security’s Security Conference and Workshop.

  Impact: BTF participation in this event assists in cross-agency communication about biometric solutions and gives members of both agencies the same baseline biometrics knowledge and lexicon.

SUPPORT FOR OUTSIDE AGENCIES

The FBI asked the BTF to assist in providing still photographs of biometrics in use in DoD. The FBI is building a short video to showcase proposed uses of their Next Generation Identification System. The BTF, with help from G-2, PM Biometrics, and the USMC liaison to the BTF, responded with 30 images of biometric data being collected in DoD.

Impact: Quickly responding to outside agency requests helps solidify the working relationship between the FBI and the BTF and serves as a means to showcase DoD biometric activities through their outreach methods.

WEBSITE

The BTF public website was updated for the first time since spring 2006. This major revamp included logo and layout changes to reflect organizational changes in the BTF. The public website is readily accessible by the general public, and it now reinforces the strategic message of the BTF.

Impact: This update makes the website more user-friendly and more dynamic in keeping with Defense Science Board recommendations. It is also now easier for BTF personnel to keep material updated on the site.

TECHNICAL INTEGRATION DIVISION

THE TECHNICAL INTEGRATION DIVISION

The Technical Integration Division is responsible for coordinating the development and consolidation of national and international biometric standards, the Joint Capabilities Integration and Development System (JCIDS) and requirements development process for DoD biometrics, and the enterprise architecture of DoD biometric systems and processes. This division assists policy planning, responds to requests for information from forward-deployed biometrics Torch Parties, and coordinates joint, interagency, non-governmental, and international biometric efforts.

STANDARDS BRANCH

BACKGROUND

The Standards branch leads BTF efforts to develop and adopt high-priority biometric standards, participate in standards development organizations and interagency forums, and develop biometric testing methodologies and tools in support of DoD mission requirements and in coordination with the DoD and U.S. government (USG) agencies.

ACCOMPLISHMENTS

MEMBERSHIP IN INTERNATIONAL STANDARDS BODIES

The BTF participated as an active member in meetings of the National Biometrics Standards Body (INCITS M1) and the U.S. Expert delegation to the International Biometric Standards Body (JTC 1/SC 37). The BTF is also a member of the Organization for the Advancement of Structured Information Standards (OASIS) and participates regularly in workshops of the National Institute of Standards and Technology (NIST) Information Technology Lab (ITL). FY07 BTF participation in these biometric standards bodies included serving as editor of six national and international biometric standards (three of which were published), developing 17 technical contributions, and responding to 21 letter ballots and 22 public reviews.

The BTF also developed and promulgated the DoD Electronic Biometric Transmission Specification (EBTS) version 1.2, which contains resolutions to 17 submitted change requests. EBTS is the mandated transmission specification that facilitates the exchange of biometric data with the DoD ABIS, provides for partial interoperability with the FBI IAFIS, and will facilitate data exchange with the Next Generation DoD ABIS (NGA). The BTF Standards team will soon complete the development and promulgation of DoD EBTS version 2.0.

Impact: Contributing to national and international biometric standards allows the BTF and DoD to influence and ensure timely development of high-priority, mission-critical biometric standards.

DOD BIOMETRIC STANDARDS WORKING GROUP (BSWG)

The BTF chaired and supported six meetings of the BSWG. The BTF also prepared six publicly available activities and standards development status update documents, which provide a consolidated view of BTF activities related to the development, adoption, and tracking of various standards-related projects. BSWG membership consists of representatives from joint, interagency government organizations, and academia, including but not limited to U.S. Army, U.S. Air Force, U.S. Navy, U.S. Coast Guard, U.S. Marine Corps, Defense Information Systems Agency (DISA), Defense Intelligence Agency (DIA), Defense Manpower Data Center (DMDC), NIST, FBI, and DHS. The BSWG is the primary forum that leads, consolidates, and coordinates biometric standards development, adoption, and implementation activities within DoD and across the USG.

Impact: BTF leadership and participation ensures that standards activities are consistent with other efforts and the strategic direction for biometrics in DoD.

ADOPTION OF STANDARDS

The BTF, in coordination with the BSWG, led the adoption of three national biometric standards and proposed for adoption 11 national and international information technology (IT) biometric standards within the DoD IT Standards Registry (DISR), which is maintained by DISA. In addition, the BTF and NIST served as co-editors of a National Science and Technology Council (NSTC) report on USG use of biometric standards, which was published on biometrics.gov. The BTF consolidated input from several Federal organizations, including DoD, DHS, NIST, FBI, National Counterterrorism Center (NCTC), and the Intelligence Community to develop this policy document, which contains technical and policy recommendations on the use of biometric standards within the USG. This policy document describes a strategy regarding USG biometric standards activities to support both interoperable government systems and broader national needs.

Impact: This policy document provides general guidance on the use of standards for biometric operations and assigns responsibilities to the NSTC Biometric Standards & Conformity Assessment Work Group (SCA WG) and member agencies.

STANDARDS OUTREACH EFFORTS

The BTF leads DoD efforts in research, analysis, and development of quality measurement algorithms and tools and regularly participates in industry events focused on cutting-edge biometric technologies. The BTF developed and evaluated Image Quality Measurement algorithms and corresponding toolsets for finger and face modalities. For those modalities, the development of quality algorithms and initial working prototypes was completed. The Finger Image Quality Measurement algorithm was published in the Journal of Forensic Identification, Vol. 57, No. 2, March/April 2007. Measuring the quality of biometric samples is a crucial step in the enrollment and identification processes. Field operators need to quickly have an algorithm that provides calculated quality scores from collected images to assist them in rendering accept or reject decisions. NIST will perform large-scale testing of both BTF quality measurement tools to evaluate performance and limitations and establish biometric sample quality minimum criteria.
In FY07, the BTF participated in a number of seminars and conferences.
In September 2007 alone, the BTF participated in the Second National Biometric Challenge Workshop hosted by the International Biometrics Industry Association (IBIA), briefed an overview of DoD mobile devices at the NIST XML (eXtensible Markup Language) and Mobile Identification Workshop, and participated in seminars of the First International Conference on Biometrics: Theory, Applications, and Systems, sponsored by the Institute of Electrical and Electronics Engineers (IEEE). BTF participation in such industry-wide forums and biometric standards bodies is part of a continuing effort to ensure DoD interests are addressed and protected during development of interoperable biometric systems and the overall biometrics enterprise.

Impact: The development of biometrics quality measurement tools and participation and presentations at biometrics workshops and conferences demonstrate that the BTF is at the forefront of biometrics technology development.

ARCHITECTURE BRANCH

BACKGROUND

The development of an architecture for biometrics is a critical component for efficient and effective operations. The Architecture branch works with stakeholders in the biometrics community across DoD to develop enterprise and mission area/domain architectures based on user-required capabilities upon which to build new biometric-enabled systems. Through active participation with operational leadership in theater and systems developers in joint forums, the Architecture branch serves as the integrating element to align biometric resources and required biometric capabilities and ensure that biometric-enabled systems can share information among DoD, other USG Departments, and our international partners.

ACCOMPLISHMENTS

COORDINATION ACROSS DOD ORGANIZATIONS

The BTF participated with PM Biometrics to review the technical approach presentation of the Northrop Grumman Stakeholder Advisory Group (SAG) for the Integrated, Enterprise Biometrics Contract in support of the U.S. Central Command (CENTCOM) Enterprise Joint Urgent Operational Needs Statement (JUONS). This was a critical first step to ensure participation and support of key stakeholders across DoD. The BTF provided leadership to the working group to support the NATO International Security Assistance Force (ISAF) in Afghanistan withbiometric collection and exploitation capability and reviewed status and issues for deployment, support, and operations to ISAF using the Biometrics Automated Toolset (BAT) solution. In addition, the BTF, in conjunction with the Army CIO/G-6, created the Biometric Data Sharing (BDS) Community of Interest (COI). The BDS COI established a joint forum, the Biometric Working Integrated Product Team, to develop and implement the Biometric Core Data Glossary, Integrated Biometric Data Dictionary, Biometric Systems Gap Analysis, the Biometric Enterprise Data Model, and the development of a portal, which is the DoD Biometric expert knowledge system designed to maintain a repository for architecture and analysis products in order to support the biometrics community.

Impact: These efforts led to the successful ISAF implementation and operation of BAT and Handheld Interagency Identity Detection Equipment (HIIDE) systems that contributed directly to support of ISAF and NATO forces. These products will assist the DoD/USG biometric communities to share data across multiple mission areas and domains. Also, these products will act as the initial biometric enterprise products that will provide the data road map for JCIDS documentation of biometric systems.

DATA TRANSFER BETWEEN NGIC AND ABIS

The BTF joined with the Joint Chief of Staff J6 to initiate the effort to place a Cross Domain Solution (CDS)/Multi-Level Security data guard capability at the National Ground Intelligence Center (NGIC) to provide two-way data transfer (SIPR to NIPR and NIPR to SIPR) with the Automated Biometric Identification System (ABIS) at the Biometrics Fusion Center.

Impact: This forum aided in the development of EA strategy to integrate architectural efforts for biometrics at the enterprise and Service level.

ARCHITECTURE IN THEATER

Efforts to operationalize biometrics in theater included the "Torch Team," a leave-behind group of individuals solely dedicated to biometric systems and process improvement/support. Additional support consisted of development of a biometrics Concept of Operations (CONOPS) (the CENTCOM CONOPS vs. the Enterprise-level CONOPS), as well as participation in the CENTCOM Architecture and Biometrics Conference at Camp Sayliyah, Qatar. In conjunction with the Army CIO/G-6 , the BTF established the Joint Biometric Architecture Working Group (JBAWG). The JBAWG was responsible for developing the Forward Operating Base/Brigade Combat Team Biometric Enabled Identity Superiority Architecture, developing the architecture products required as part of the Biometrics Enterprise Core Capabilities (BECC) Capabilities Production Document (CPD), and will develop the Biometric-Enabled Identity Superiority Architecture/DoD Biometric Architecture.

Impact: These architecture products serve as visible, direct, and enduring support to forces deployed in-theater, help align biometric resources and biometric required capabilities contained in the Biometric Joint Capabilities Integration and Development System (JCIDS) strategy, manage the DoD Biometric portfolio of capabilities/systems, and share biometric data across DoD, USG, and with our international partners.

REQUIREMENTS BRANCH

BACKGROUND

The purpose of the Requirements branch is to gather and validate operational and technical requirements and resolve stakeholder issues that affect the joint biometrics enterprise. Additionally, the Requirements branch supports the bio-metrics governance process through varied forums as a single establishment for identifying common biometric requirements and submitting them for Joint Requirements Oversight Council (JROC) validation. The biometric requirements process is not intended to replace traditional requirements validation processes. However, no specific resources within the BTF are required to support acquisition management.

ACCOMPLISHMENTS

BIOMETRICS EXECUTIVE COMMITTEE

The BTF supported the preparation and coordination of material for the Biometrics Executive Committee (EXCOM), a senior-level body which is chaired by a four-star flag officer/SES equivalent. It assisted in the construction of a presentation depicting Joint Required Operational Capability (JROC) Biometrics priorities and the actions being taken to enable capabilities, funding to be applied and schedule of distribution, and outlining any issues for decision consideration.

Impact: The BTF supports the EXCOM in the execution of the Deputy Secretary of Defense (DepSecDef) memorandum dated 4 Oct 2006, "Defense Biometrics," which is charged with ensuring "…timely and vigorous action on biometrics-related activities across the Department.…" The BTF governance structure as executed supports the Biometrics EXCOM to accomplish its charter.

JOINT BIOMETRICS SENIOR EXECUTIVE STEERING COMMITTEE (JBSESC)

The BTF administers the JBSESC in the coordination of material for the Biometrics Executive Committee. The Joint Biometrics Senior Executive Steering Committee is chaired by the Director, BTF and Director, Defense Biometrics with participants at the two-star general officer/SES equivalent level. It assisted in the refinement of requirements for the FY08 biometrics budget submission and the establishment of a working group to review base access requirements for decision consideration.

Impact: The BTF as the JBSESC administrative element, provided support to the EXCOM with research and coordination to provide refined decision items to the EXCOM. This senior-level support assists in ensuring the specific aspects of biometrics requirements are clearly defined and addressed as early as possibly in the decision process.

JOINT BIOMETRICS OPERATIONAL COORDINATION BOARD (JBOCB)

The JBOCB is an Action Officer-level collaborative body that incorporates all DoD Biometrics community stakeholders, to include Combatant Commands (COCOMs), Services, agencies, Joint Staff, and OSD. Interagency partners are invited to attend as supporting members. It is the initial entry forum that is one of four voting bodies that constitute the larger Joint Biometrics Governance Structure.

Impact: The JBOCB has developed, coordinated, and executed FY07 requirements to support biometrics functions of collect, match, store, and share across DoD and some limited interagency, as well as multi-national offices. Through the support of this forum biometrics has created a process to review requirements across the full-spectrum of Warfighter needs.

SUPPORT TO JOINT BIOMETRICS TECHNICAL COORDINATION BOARD (JBTCB)

The Requirements branch team led a review of the governance process for the JBTCB outlined in the charter to clarify the submission process of matters determined by the JBOCB through the change request (CR) process. These requests would be further defined to provide the technical solution, timeline for production, and funding solution.

Impact: The BRF through the JBOCB directs the JBTCB as the technical arm of the biometrics governance structure to develop and coordinate the technical analysis of proposed requirements addressing cost, schedule, and performance. Through this process, the biometric requirements are met with efficiency and effectiveness to the Warfighter.

JOINT, INTERAGENCY, MULTINATIONAL COLLABORATION

BACKGROUND

The BTF works directly with representatives from the Armed Services and other government agencies to develop and implement biometric technologies on the ground. In addition to work done jointly with the FBI and DHS, the BTF has been working with the U.S. Marine Corps (USMC) and the Navy on a number of different projects.

USMC LIAISON ACTIVITIES

The BTF and the USMC have maintained a close working relationship since 2005 when the USMC established a liaison position at the BTF. Since that time, the USMC has added four contract support positions to handle the fast-paced and challenging demands of the emerging DoD Identity Management enterprise.

ACCOMPLISHMENTS

Training: Fielded BAT and HIIDE training elements at the Marine Air-Ground Task Force (MAGTF) Integrated Systems Training Centers (MISTC) at each Marine Expeditionary Force (MEF), Camp Lejeune, Camp Pendleton, and Camp Butler.

Impact: This robust training capability provides MEF Commanders with the ability to train units and personnel on current biometric systems prior to deploying in support of Operation Iraqi Freedom (OIF) and Operation Enduring Freedom (OEF). This training capability directly supports biometric training requirements as outlined by a November 2007 Multinational Forces - Iraq (MNF-I) Strategic Operations Memorandum.

Training: The USMC corrections specialist school, a Military Occupational Specialty (MOS) producing school at Lackland AFB, was provided six BAT clients and two HIIDEs to incorporate this training into the course curriculum for the Corrections MOS.

Impact: Enhanced Training Capability of the Marine Corrections Detachment ensures that Corrections Specialists are properly trained on biometric-enabled systems prior to deployment and assumption of enemy detainee missions. BAT and HIIDE instruction is now part of the curriculum for the Corrections MOS.

Training: Deployed 20 BAT and 24 HIIDE devices with field support engineers to the mission rehearsal exercise Mojave Viper.

Impact: Biometrics are now taught and integrated throughout the exercise, which enhances Mojave Viper and provides a more realistic training environment prior to deployment. Marine units have the opportunity to train, demonstrate expertise, and develop the Tactics, Techniques and Procedures (TTPs) that they will be using in theater prior to deploying.

Operations: Integrated BAT and HIIDE capability and training into the 22nd Marine Expeditionary Unit (MEU) pre-deployment work-up. Further, the 22nd MEU conducted the first-ever biometric data refresh while underway, using shipboard organic communications. The USMC is exploring the expansion of a biometric-enabled operations capability for other MEUs.

Impact: This training and capability ensures that forward-deployed Marines have the latest biometric-enabled capability and identity management tools available while they are afloat. It provides the MEU Commander with the ability to conduct identity superiority operations in any climate and place.

Operations: Deploying 17 biometrics field support engineers (contractors) to operate in theater in support of biometrics at the Battalion level. These individuals will be responsible for local training, maintaining, and limited repair of biometric equipment within units assigned to Multinational Forces – West (MNF-W).

Impact: The employment of complex and sophisticated biometric-enabled systems required additional skill set support beyond that available in the MOS inventory. These support personnel are deemed critical to optimization of biometric-enabled systems in theater.

Requirements: The Office of the Chief of Naval Operations (OPNAV) N86, in concert with the USMC, developed a Capability Development Document (CDD) for the Identity Dominance System (IDS). IDS is a materiel solution for biometric collection and verification with both hardware and software components that provide a multimodal biometric capability to match the optimum biometric and data structure to each user's mission profile. The system includes ancillary equipment such as cameras and scanners. IDS is interoperable with a variety of other systems and adheres to applicable technical standards and policies, including the DoD Electronic Biometric Transmission Specification (EBTS) and network security accreditation. The BTF has supported the USMC in the development of the IDS CDD by providing document reviews, recommendations, and significant support in resolving Joint Staff review comments.

Impact: IDS will represent the next step in biometric collection capabilities, ushering in the next generation of collection equipment utilizing lessons learned and correcting shortfalls of previous or existing hardware and software.

Operations: Working with the Joint Chiefs of Staff, USN, BFC, and the Naval Criminal Investigative Service (NCIS), established a forensic Latent Print Laboratory at Camp Fallujah, Iraq. The laboratory receives, examines, and recovers latent fingerprints from commonly submitted items such as small arms and rocket launchers from caches, suspected sniper events and sites of attacks, recovered documents, and improvised explosive devices (IEDs).

Impact: These efforts have identified hundreds of individuals as scientifically linked with the item and event in question, thereby establishing a connection that can be used for criminal prosecution, intelligence targeting, or both. The laboratory submits recovered fingerprints to the ABIS to obtain matches from various databases containing fingerprint information. Matches found in the databases are passed along to the intelligence community and criminal investigation community for actions to bring criminals and terrorists to justice.

Operations: Working from requirements established by the quick-turn capabilities-based assessment team, Department of the Navy has been named the office of primary responsibility for the establishment of the Joint Expeditionary Forensic Facilities.

Impact: Will provide enhancements to existing forensic capabilities in theater as well as additional forensic capabilities.

Training: The USMC has partnered with Technical Support Working Group to produce a standardized "Joint" template for Sensitive Site Exploitation training curriculum and an associated support package. The SSE training support package will be completed by January 2008. Inputs have been received from U.S. Army Criminal Investigation Laboratory (USACIL), NCIS, NGIC, and interagency organizations.

Impact: Will provide standardized training to Soldiers, Sailors, Airmen, and Marines collecting exploitable items for prosecution and/or intelligence purposes.

U.S. NAVY LIAISON ACTIVITIES

The BTF and the U.S. Navy (USN) have maintained a close working relationship since 2000 when the Navy established a liaison at the BTF. The liaison has worked to ensure Navy projects meet DoD Biometrics Enterprise requirements through standardized protocols and interoperability standards.

ACCOMPLISHMENTS

EXPANDED MARITIME INTERCEPTION OPERATIONS

The USN began using biometrics in FY07 to help identify persons of interest aboard commercial vessels. USN ships operating in the U.S. Central Command (CENTCOM) Area of Responsibility (AOR) have the capability to collect and forward biometric data collected from potential terrorists for searching against databases. These operations, referred to as Expanded Maritime Interception Operations (EMIO), are part of the Navy's Vessel Boarding Search and Seizure (VBSS) program.

The establishment of EMIO biometrics was no small achievement. It required the BFC to work closely with the Navy to identify biometric collection equipment, develop data transmission standards, and help establish procedures. The ABIS provides the Navy with near-real-time database search results.

Impact: As EMIO-capable ships are brought on line, the BFC provides up-front coordination to register the ships prior to the Navy's submission of operational data. The BFC provided valuable assistance to the Navy in recommending EMIO biometric collection equipment and conducting testing to ensure compatibility with data standards required by ABIS.

EMIO Wireless Bridge

Biometric data collected from passengers and crew of an intercepted merchant ship during EMIO operations must be forwarded to the BFC for searching against the ABIS database. There is a requirement to wirelessly transmit the biometric data to the host USN vessel for relaying to the BFC. Navy developers of an EMIO Wireless Bridge have worked closely with the BFC to ensure compatibility of EMIO biometric data with ABIS. The BFC has provided support to the wireless initiative by conducting proof- of-concept testing with the USS Ingraham and through participation in laboratory and ship testing with Navy developers.

Impact: More than 30 ship installations of the EMIO Wireless Bridge have been funded through the BTF.

Tactical Biometric Collection and Matching System

Early EMIO biometric collection equipment was configured from off-the-shelf components that were available at the time. EMIO boarding parties reported that the equipment was too heavy and difficult to operate and maintain. The BTF provided funds to the Navy to develop a smaller, lighter, ruggedized system with improved capability. Prototype models of a new biometric collection and verification system, named the Tactical Biometric Collection and Matching System (TBCMS),were delivered in FY07. The BFC provided technical advice to the Navy during development of the TBCMS and conducted laboratory testing to ensure compatibility with ABIS.

Impact: Funds provided by the BTF enabled the Navy to develop eight prototype TBCMS models, which will undergo extensive field testing and serve as the basis for development of pre-production models.

Identity Dominance System

The Office of the Chief of Naval Operations (OPNAV) N86 has developed a Capability Development Document (CDD) for the Identity Dominance System (IDS). IDS is a materiel solution for biometric collection and verification with both hardware and software components that provide a multimodal biometric capability to match the optimum biometric and data structure to each user's mission profile. The system includes ancillary equipment, such as cameras and scanners. IDS is interoperable with a variety of other systems and adheres to applicable technical standards and policies, to include the DoD Electronic Biometric Transmission Specification (EBTS) and network security accreditation. The BTF has supported the Navy in the development of the IDS CDD by providing document reviews, recommendations, and significant support in resolving Joint Staff review comments received from Army elements.

Impact: Support provided by the BTF has helped the Navy move the CDD through the Joint Capabilities Integration and Development System (JCIDS) process, ensuring that other Services have knowledge of the IDS and can leverage its capabilities as appropriate.

Friendly Personnel Biometrics Repository

The BTF is sponsoring the development of a Friendly Personnel Biometrics Repository (FPBR), which is part of the Naval Identity Management Development and Operations Capability (NIMDOC) initiative. Development of FPBR will be a cooperative effort between the Navy and the BFC with the objective of demonstrating access control functionality with the Defense Manpower Data Center (DMDC). The FPBR will serve as a biometrics repository for Naval employees, and the development will include participation from the Air Force.

Impact: Funds provided by the BTF will enable the Navy to develop a working model FPBR in 2008. This model will serve as a basis for other Services' applications in the area of friendly personnel biometrics.

Forensics

Working with the Joint Chiefs of Staff, USMC, and the BFC, the Naval Criminal Investigative Service (NCIS) established a forensic Latent Print Laboratory at Camp Fallujah, Iraq. The laboratory receives, examines, and recovers latent fingerprints from commonly submitted items such as small arms and rocket launchers from caches, suspected sniper events and sites of attacks, recovered documents, and IEDs. These efforts have identified hundreds of individuals as scientifically linked with these types of events, thereby establishing connections that can be used for criminal prosecutions and intelligence targeting. The laboratory submits recovered fingerprints to the ABIS to obtain matches from various databases containing fingerprint information. Matches found in the databases are passed along to the intelligence community and criminal investigation community for actions to bring criminals and terrorists to justice. Working from requirements established by CENTCOM, the BTF has fully supported plans to expand NCIS forensic capabilities in the AOR.

Impact: Forensic enhancements in the AOR that have been funded through the BTF include the addition of three lab facilities, development of a new modular lab concept, and establishment of lab manning and sustainment procedures to enable 12/7 operations.

JOINT INTEROPERABILITY TEST COMMAND (JITC) LIAISON ACTIVITIES

The BTF has maintained a close and sustained partnership with the JITC since March of 2002. The partnership stems from a Smart Card Senior Coordinating Group (SCSCG) requirement to investigate the use of biometrics in conjunction with the DoD Common Access Card (CAC). JITC provided Test and Evaluation (T&E) expertise to include the development of test plans, test reports, and test execution in support of four technology demonstrations. With the expansion of biometric technologies and systems in conducting the Global War on Terrorism, interoperability of biometric systems within the DoD became paramount. In 2004, JITC was requested to provide an on-site interoperability liaison at the BFC in an effort to improve data sharing activities for DoD biometric systems.

ACCOMPLISHMENTS

In 2007, the BTF partnered with JITC in support of collective T&E efforts with the BFC and other test agencies to ensure that all interoperability requirements are met.

Impact: Combining test efforts and resources minimizes impact to overall program schedule and cost.

Initiated standards conformance certification memorandums for the Biometric Identification System for Access (BISA), the U.S. Special Operations Command (SOCOM) Biometric Collection and Identification Equipment (BCIE), and the Navy's Tactical Biometrics Collection and Matching System (TBCMS).

Impact: Standards conformance provides the foundation for the DoD-mandated joint interoperability certification.

Participated in ABIS integration test events that supported an interoperability assessment of the SOCOM BCIE and initiated efforts for the BISA and the TBCMS.

Impact: Supports the initial efforts for the DoD-mandated joint interoperability certification.

Provided interoperability support to the BTF/BFC through participation in high-level efforts supporting the identification of joint requirements for Defense Biometrics systems such as the U.S. Joint Forces Command (JFCOM)-led Capabilities Based Assessment (CBA). Technical support included the interoperability aspects of the Joint Staff Net Ready Key Performance Parameter (NR-KPP), Information Support Plans (ISPs), Joint Staff requirements processes, and the Net-Centric Operations and Warfare (NCOW) Reference Model. Additional efforts included support to activities such as T&E, Architecture, Standards, and Enterprise Interoperability Working Integrated Product Teams (WIPTs).

Impact: Supports the initial efforts for the DoD-mandated joint interoperability certification.

OPERATIONS DIVISION

THE OPERATIONS DIVISION

The Operations Division is responsible for establishing and synchronizing operational support activities to ensure that biometrics capabilities enable military operations and business functions.

CURRENT OPERATIONS

BACKGROUND

As currently configured, the mission of the Operations Division is threefold. First, the division is responsible for coordination and management of issues and requests for information (RFIs) from biometric cells in Iraq and Afghanistan. In this effort, it also supports and addresses all combatant command (COCOM) biometric-related requests for information. Along with this role in providing immediate Warfighter support is the division's second responsibility, which is to drive efforts throughout the Joint Force to provide comprehensive biometric training programs (i.e., operator, leader, collective, and institutional). Finally, the division is responsible for the administration of day-to-day operations within the BTF to include the management of an internal and external calendar and oversight of all internal and external activities. While the division's efforts are largely focused on near-term operations, its long-term focus is centered on the establishment of biometric organizations within all Combatant Commands, development of a framework for a corresponding world-class operations center to support worldwide biometric operations, and the institutionalization of biometric training throughout the Force.

ACCOMPLISHMENTS

In FY07, as combat operations in Iraq and Afghanistan entered their fourth and sixth years, respectively, the focus shifted toward bringing biometric technologies to the Warfighter and using them as a tool to help prevent insurgent activities. Across all doctrine, organization, training, materiel, leadership, personnel, and facilities (DOTMLPF) domains, the BTF was at the forefront of the movement to operationalize biometrics. While the BTF and the biometrics community positioned themselves to better support the Warfighter, biometric enrollments increased, and the number of detained insurgents increased exponentially during 2007. As the use and roles of biometrics continue to expand, the BTF and the biometrics community enable the conditions to provide systematic support to the Warfighter for years to come.

This is reflected in the BTF's transfer within the Army staff from the Communications, Information, and Systems Directorate (CIO/G-6) to the Training and Operations Directorate (G-3/5/7). At the highest levels of the Army and the DoD, this transfer sent the distinct message that biometrics were moving from concept to execution. In FY07, the message began to permeate throughout the Joint Force as subordinate staffs likewise transferred responsibility for biometrics into training and operations elements. In February 2007, Multi-National Corps – Iraq (MNC-I) realized the need for a dedicated staff component to tackle the daunting task of operationalizing biometrics in the Iraq theater of operations. In response, the BTF and Headquarters, Department of the Army (HQDA) G-3/5/7 deployed a Biometrics Torch Party to Iraq. Originally a five-man, joint-Service element, the Torch Party integrated itself with the Training and Operations (CJ-3) element within the MNC-I headquarters. The Torch Party, which had a 30-60-90 day mission, set its initial sights on standardizing the issuance and training of biometric devices to units, developing concepts of operations (CONOPS) and standard operating procedures (SOPs) for employment, and increasing the number of enrollments and watch list nominations.

With the BTF serving as its clearinghouse for requests for information (RFIs) and its primary reach-back organization in the United States, the Torch Party continued to expand the biometric foothold in Iraq to support the Warfighter, tackling such issues as software and communication upgrades and latent print backlogs. The Torch Party has since matured, and MNC-I and CENTCOM have recognized the importance of this organization and have submitted a joint manning document (JMD) that has since been approved by the Joint Staff and will establish a permanent 11-man biometrics cell within the MNC-I headquarters for years to come. Following the success of the Iraq Torch Party, the HQDA G-3/5/7, with BTF oversight, deployed a three-man team to Afghanistan to tackle the same tough issues within the Combined Joint Task Force – 82nd Airborne Division (CJTF-82) CJ-3 element which also resulted in the submission and subsequent approval of a JMD.

At the heart of both cells' efforts is their charter to provide units with the tools (i.e., doctrine, training, materiel, education, etc.) that they would need to increase biometric enrollments. The chief purpose for using biometrics in DoD today is to identify enemy insurgents and manage populations within a specific battlespace throughout a theater of war and around the world. To do this most efficiently, a great deal of data must be collected. As the biometrics support structure improved in FY07, so too did the number of enrollments. Armed with new tools, in a short period of time, biometric data were collected at a rate exceeding all previous years combined

Impact: Using the fingerprints that forensics teams lifted from exploded bombs, abandoned enemy sniper rifles, etc., more than 100 enemy insurgents were identified and detained in FY07.

TRAINING ACTIVITIES

BACKGROUND

At the forefront of BTF efforts to operationalize biometric capabilities in Iraq and Afghanistan has been the acceleration of training to ensure that our Soldiers, Sailors, Marines, and Airmen are prepared to use biometrics to successfully execute their missions. To that end, the BTF partnered with the Army's Training and Doctrine Command (TRADOC), the Army's Forces Command (FORSCOM), PM Biometrics, the Army Space Program Office (ASPO), and Joint Forces Command (JFCOM) to meet near-term training needs to support OIF and OEF while laying the groundwork for the long-term institutionalization of biometrics across the Joint Force.

ACCOMPLISHMENTS

Paramount to all training initiatives in FY07 has been the preparation of deploying units for their OEF/OIF missions. In accordance with a 19 Jun 07 directive from the BTF and the Army Deputy Chief of Staff for Training and Operations, TRADOC published a pre-deployment training plan, established biometrics as a focus area within the Center for Army Lessons Learned (CALL), and assigned the operations section within all subordinate Army staffs as the primary proponent for biometrics.

While TRADOC and PM Biometrics were spearheading the efforts to meet immediate Warfighter requirements, the groundwork was being laid for the institutionalization of biometrics training in the longer term. At the onset of FY07, JFCOM led a quick-look Capabilities Based Assessment (CBA) that outlined gaps and deficiencies across the spectrum of biometrics, to include five training deficiencies ranging from lack of institutional training to the lack of a biometrics military occupational specialty (MOS). The identification of these gaps set the conditions for the future institutionalization and synchronization of biometric training across the Joint Force. To properly forward biometrics throughout the Force, it is imperative that leaders be aware of the warfighting capabilities that biometrics can provide.

At the specific behest of the MNF-I Commander, GEN David Petreaus, the BTF began briefing leaders at the brigade level on biometrics as part of their mandatory Counterinsurgency Seminar.

Impact: As biometric training and leader awareness improved in FY07, so, too, did the number of enrollments. Armed with the knowledge they needed, these personnel collected and submitted more biometric data in 2007 than all previous years combined.

RESOURCES & SUPPORT DIVISION

THE RESOURCES & SUPPORT DIVISION

The Resources and Support Division establishes and synchronizes operational support to ensure that biometrics capabilities enable military operations and business functions.

BACKGROUND

The Resources & Support division and its three branches exist to implement information technology, oversee security, and manage resources throughout the BTF

ACCOMPLISHMENTS

Several efforts were undertaken in partnership with other organizations, including an effort to push latent fingerprints onto watch lists. In addition to the BTF, this effort involved NGIC, the PM, and the Fort Huachuca Language Technology Office (LTO).

SECURITY BRANCH

BACKGROUND

The BTF Security mission is to protect the BTF from a compromise of sensitive and classified information; loss of life; damage, loss, or destruction of government property; or disruption of mission. The Security team protects staff, visitors, buildings, and property by enforcing applicable laws, ordinances, and Army security policies and procedures. This includes the detection and prevention of theft, trespass, sabotage, and espionage. The Security team assists and plans for emergency situations such as assisting in the prevention of fire damage, accidents, and hazards. It prepares, enforces, and executes an Emergency Action Plan and manages all DoD and U.S. Army security programs, to include communications security (COMSEC) within the BTF.

ACCOMPLISHMENTS

S&T COORDINATION

During this past year, the BTF Security team established and upgraded visitor control procedures and the closed-circuit television and IDS systems. The team made significant strides toward the ability to issue Common Access Cards through a Defense Enrollment Eligibility Reporting System (DEERS) - Real-time Automated Personnel Identification System (RAPIDS) system that will be in place in early FY08. Team members attended monthly Anti-Terrorism/Force Protection (AT/FP) meetings with local, state, and federal agencies in addition to conducting quarterly AT/FP training scenarios with local Special Reaction Teams to practice countermeasures should the BFC building ever be compromised.

The Security manager instituted an effective security education program for guard personnel as well as BFC employees to keep them abreast of the latest initiatives, security procedures, and DoD rules, regulations, and requirements. The security office passed the annual National Security Agency COMSEC inspection and assisted the G-3 security office on a regular basis for several issues throughout the year.

Impact: Improvements in security enabled smooth data transmission and a secure data chain.

INFORMATION MANAGEMENT BRANCH

BACKGROUND

The Information Management branch is responsible for Information Technology (IT), Information Assurance (IA), and Knowledge Management (KM) for the BTF and BFC.

ACCOMPLISHMENTS

The Information Technology team (NetOps) not only continued to provide comprehensive services to the programs and users that rely on our networks during FY07 with zero unplanned outages and an up-time rate of over 99.5%, but also considerably expanded BTF and BFC network capabilities.

The primary challenge in FY07 was to appropriately acquire, configure, and utilize approximately $4.4 million in equipment purchased with FY06 end-of-year money. Leadership's vision has long been to permanently establish the DoD Biometrics Domain separate from any one Service in the manner of the Defense Manpower Data Center (DMDC) and other similar organizations. The much needed $4.4 million in end-of-year funds allowed for the purchase of specialty hardware, software, and systems specifically for that purpose. The configuration and implementation rate is at approximately 65 percent. Staff shortages have been and will continue to be the major contributor to implementation delays.

Impact: The extensive equipment additions, notable staff expertise, and recent bandwidth increases will enable a dynamic, agile, and robust domain that meets the information sharing requirements of the DoD as well as our federal and Coalition mission partners.

The IA team significantly increased the security posture of the DoD Biometrics networks and operations during FY07 with the addition of a wide variety of IA tools and hardware. An architecture redesign, which better segregated ABIS, BISA, Development, Research, and Web Services, was also completed. Additionally, the BFC's Configuration Management (CM) process was reviewed and expanded during FY07.

Impact: The redesign allows for tighter controls and more expansion flexibility. Structured CM improvements allow for easier certification & accreditation updates, particularly for our Defense Information Certification and Accrediation Process (DIACAP) System Security Authorization Agreements (SSAAs).

These and other improvements allow for better mission assurance, information sharing, and information assurance on trusted, interoperable networks.

The Knowledge Management (KM) team made great strides in centralizing and consolidating KM for the organization. The security framework for the DoD Biometrics Expert Knowledge System (DBEKS) was completed and deployed in FY07 to the benefit of all operational and business web services. DBEKS is the secure portal for DoD Biometrics, and the security framework provides enhanced user features such as single-sign-on and the ability to change account information, e.g., passwords and e-mail addresses, via automation. Many KM components were successfully migrated to the new framework during FY07, with the following currently in place: Data Sharing COI, CIO Library, Document Request Form, IDProTECT-NIMDOC Coordination Website, Mass Mailer, Requirements COI, Resource Management, RM Data Sharing, Strategy Division, and T&E Reports. Many more are planned for FY08, as the KM team continues to centralize and expand BTF and BFC KM capabilities.

Impact: The new framework enhances the security posture of DoD Biometrics' web services, brings the BTF/BFC more completely into compliance with DoD Directives, and significantly reduces the manual user administration process for the help desk.

TECHNICAL MANAGEMENT DIVISION

THE TECHNICAL MANAGEMENT DIVISION

The Technical Management Division is responsible for establishing, operating and protecting DoD authoritative biometrics data, to ensure its integrity and availability for U.S. government users. The Division seeks to integrate required interface control, systems management, examination services and evaluation and assessment activities.

STANDARDIZATION, EVALUATION, AND ASSESSMENT LABORATORY (SEAL)

BACKGROUND

The Standardization, Evaluation, and Assessment (SE&A) team exists to evaluate the nation's investments in biometric-enabled information technology (IT), programs, and product support necessary to support the federal government. In that context, the continued objective is to rapidly test quality biometric products that satisfy user needs with measurable improvements to mission capability. The team focuses on ensuring biometric systems deployed are functional, standards-conformant, and interoperable with ABIS, the DoD's authoritative database. SE&A is the key safeguard to ensure data ingested by ABIS will not corrupt its database or other repositories of biometric data.

To accomplish this task for the biometrics Community of Interest (COI), the SE&A team works with other test agencies and evaluates all biometric-enabled IT devices or systems. The core increment of a biometric-enabled IT device or system provides the basic infrastructure necessary to support ensuing incremental functionality and consists of basic hardware, system software and tools, and fundamental applications. The core increment is considered a militarily useful and supportable capability effectively defined, developed, deployed, and sustained as an integrated entity or as a building block of a target system. Ensuing increments may be composed of one or more spirals or other developmental elements where each successive increment builds upon the capabilities and functionality previously deployed.

DoD Instruction 5000.2, "Operation of the Defense Acquisition System," requires that SE&A programs be structured to provide accurate, timely, and essential information to decision makers for programs throughout the system lifecycle. As the means to this goal, SE&A identifies and learns about deficiencies (technical or operational) so that they can be resolved prior to production and deployment.

ACCOMPLISHMENTS

The SE&A team reached important milestones in FY07. For more than three years, SE&A has operated a test framework that established a legacy of innovation and entrepreneurial growth. For the third consecutive year, SE&A exceeded its goal for number of test events conducted. During the past fiscal year, SE&A conducted 32 test events. These test events supported PM Biometrics, the Naval Innovation Laboratory (NaIL), Army G-2, and others.

Impact: BFC testing ensured that more than 900 new systems deployed to support Operation Iraqi Freedom and Operation Enduring Freedom met operational needs and that data collected were shared with the DoD authoritative biometric database and other databases as appropriate.

The SE&A team evaluated biometric-enabled IT products, programs, and services during Joint Force and Service-related exercises and experiments, most notably the Tactical Network Topology (TNT) exercises. The team identified capability-focused, effects-based processes to improve performance, interoperability, and supportability for both materiel (acquisition or procurement) and non-materiel (Doctrine, Organization, Training, Material, Leadership and education, Personnel, and Facilities (DOTMLPF)) solution sets. The SE&A team's success is a tribute to its hard work, innovative nature of the staff, and partnership between contractors and government personnel.

Impact: The SE&A team identified numerous tactical capabilities and limitations in Special Operations Forces biometric collection and matching processes. Event and system findings were fed through the Joint Training System, Joint Warfighting Capability Assessment process, Functional Capabilities Boards, and SOCOM for remediation and DOTMLPF analysis of future capability needs.

Throughout FY07, the SE&A team created 145 Emerging Results Reports (ERRs) to support events and various exercises. The ERRs are supplied to government, developers, and integrators to summarize activities conducted during events and provide raw data to be analyzed prior to the issuance of a final report.

Impact: To help transform the way the DoD collects, analyzes, and disseminates mission-critical biometric information, the SE&A team worked with program managers and developers of the Biometrics Automated Toolset (BAT), Biometric Identification System for Access (BISA), Defense Biometrics Identification System (DBIDS), Tactical Biometric Collection and Matching System (TBCMS), and Handheld Interagency Identity Detection Equipment (HIIDE) to improve their abilities to collect, store, match, transmit, and manipulate biometric and biographic data.

The SE&A team is developing a more collaborative, efficient, and disciplined team with the tools and training to scale to larger programs and refine its standards conformance capability. With the addition of four personnel, The branch is reinvigorating its Commercial Off-The-Shelf (COTS) and Government Off-The-Shelf (GOTS) product evaluation tasks, researching laboratory accreditation needs, and seeking to validate and verify the BFC modeling and simulation capability. The team has networked with several Operational Test Agencies to include the Army Test and Evaluation Command (ATEC), the Joint Interoperability Test Command (JITC), and the Navy Operational Test and Evaluation Forces (OPTEVFOR) to institutionalize test efforts. This spirit of collaboration helped SE&A reach another important milestone — completion of the first BFC-JITC collaborative standards conformance event.

Impact: These actions will provide an operationally realistic environment for vendors, customers, and decision makers to interact with a myriad of biometric technologies. This environment will provide the framework necessary to ensure that future biometric solutions are functional, standards-conformant, and interoperate with the ABIS, the DoD's authoritative database, and other repositories of biometric data.

FACILITIES INITIATIVES

BACKGROUND

Legislation authorizing DoD initiation of biometric activities came into effect in 2000. Initial facilities to support these activities were secured through small General Services Administration leases in the Clarksburg, W.Va., area. Over time, the nature of DoD biometric efforts has become more sensitive, and the concern for terrorist activity, after the attacks of 9/11, has increased. As a result, the long-term facility strategy has been to co-locate with the FBI Criminal Justice Information Services (CJIS) Division at its approximately 1,000-acre installation in Clarksburg, W.Va. The initial effort was to do this as a DoD stand-alone facility on this installation.

ACCOMPLISHMENTS

During FY07, the facility strategy for defense biometrics changed from consolidating West Virginia operations into a stand-alone facility on the FBI CJIS installation to a joint FBI-DoD facility at the same location. While the DoD was developing plans for the stand-alone facility, the FBI activated its plans to build additional facilities and agreed to combine efforts with the DoD. This is planned in the FY10 Military Construction program, with occupation scheduled for FY12. Economies of scale and synergies from partnering with the FBI for biometric facilities are significant. The process to select a design firm and initiate the design began near the end of FY07.

DoD funding for the DoD portion of the project is programmed while the FBI portion awaits FY08/09 funding streams. Should the FBI not be able to continue with the joint facility project, the stand-alone facility remains the contingency plan for DoD facilities supporting biometric operations.

Impact: An effective and efficient facility plan has been put in place with programmed funding to support DoD biometric operations into the future. This action ensures that a highly reliable and well protected facility will be available in FY12 to support the vision.

PROJECT MANAGER (PM) BIOMETRICS ACTIVITIES

BACKGROUND

The Office of the PM Biometrics designs, engineers, develops, acquires, deploys, and sustains an enterprise biometric system and family of systems configurable for multiple operational mission environments, enabling identity dominance across the DoD.

The Department of the Army has designated the Army G-3/5/7 as the Executive Agent for all of DoD biometrics. The PM, under the Program Executive Office, Enterprise Information (PEO EIS), leads acquisition programs in support of the BTF. The collaborative effort exists to provide an enterprise biometric solution that best supports the joint Warfighter in achieving identity dominance.

Activities are organized around strategic goals associated with major increments of the DoD Biometrics Enterprise Roadmap.

- Maintaining ongoing biometric operations in the current environment
- Developing a near-term Enterprise Solution and enhancements to current systems that address approved U.S. Central Command (CENTCOM) Joint Urgent Operational Needs Statements (JUONS) and biometrics Quick-Look Capabilities Based Assessment (CBA) findings
- Institutionalizing biometrics by laying the technical and management foundation for disciplined materiel acquisition of an objective enterprise solution.

PM Biometrics is responsible for the operation and maintenance (O&M) of the BAT, the BISA, and the prototype DoD Automated Biometric Identification System (ABIS), which is the DoD's authoritative biometric data repository and matching system. PM Biometrics is fully committed to maintaining responsive support from these systems while improved capabilities are developed.

In addition, PM Biometrics has instituted and maintains theater support with a PM Forward organization in Iraq and a biometrics cell in Afghanistan in support of joint Warfighter operations.

ACCOMPLISHMENTS

NEXT GENERATION ABIS (NGA)

PM Biometrics awarded an integration contract for both ABIS and NGA to consolidate efforts and contracts and to provide a way ahead for the biometric System of Systems. PM Biometrics developed performance metrics that drew attention to communication issues in the CENTCOM AOR, identifying the need for an end-to-end study. Now in its second phase, this study has already supplied diagnostic metrics to stakeholders.

Impact: The end-to-end study will recommend improvements to current network operations supporting biometric tools and applications for the Army at its ABIS facility in West Virginia, the National Ground Intelligence Center (NGIC) in Charlottesville, Va., DoD and civilian agencies in CONUS, and nations within the CENTCOM Area of Responsibility (AOR) to analyze and optimize local biometric systems communication processes and make recommendations for long-term improvement.

DEVELOPMENT OF THE DOD BIOMETRIC SECURITY CLASSIFICATION GUIDE

The field of biometrics continues as an evolving set of data and processes throughout DoD. As such, a consolidated and coordinated set of guidelines for biometric data is required to avoid conflict among DoD activities and data classifications. PM Biometrics is developing the DoD Biometric Security Classification Guide (SCG) to provide instruction and guidance for the class-ification, creation, and distribution of DoD biometric information.

Impact: The SCG addresses security measures to safeguard current biometric information and development efforts within the biometric community that require ongoing protective measures.

FAMILY OF SYSTEMS (FoS)

As part of the development of the Next Generation ABIS, PM Biometrics initiated the development of the FoS for all biometric collection systems. This effort entails software development and the selection of hardware through a hardware fly-off process. To aid hardware vendors in complying with the collection and data transaction requirements of the enterprise, a Software Development Kit (SDK) and Application Programming Interface (API), along with sample applications (for SDK/API validation), are being developed within the FoS. The FoS SDK/API software will facilitate the construction of biometrically enabled end user applications that will fully integrate with the DoD Biometrics Enterprise Service Oriented Architecture (SOA). Hardware vendors will then utilize the SDK/API to develop software applications for their specific hardware collection devices, which will be evaluated through the hardware fly-off process for enterprise-wide selection and utilization. Nineteen vendors able to provide handheld capabilities were identified in a July 2007 market research effort.

Impact: FoS software is being designed and developed to provide the common hardware and software that will allow various mission-specific applications to be biometrically enabled and to fully participate in the DoD biometric enterprise. The SDK and API will bring platform and device independence to mission-specific applications and biometric service providers (using software and hardware). The July 2007 market research identified multiple vendors that meet at least 85% of DoD requirements. Multiple hardware vendors are moving forward with the development of multimodal handheld devices identified in this market research effort.

eSECURITY

In April 2006, U.S. Military Entrance Processing Command (MEPCOM) requested that PM Biometrics assist in providing acquisition support for its eSecurity project. The eSecurity project is an all-encompassing project to use face and fingerprint biometrics to tightly control enlistment into the U.S. Armed Services.

Impact: With the fielding of e-Security, MEPCOM will have a model to improve the integrity of the military enrollment process at Military Entrance Processing Station (MEPS) and Military Entrance Testing (MET) sites. The impact of e-Security implementation is DoD-wide and includes fewer fraudulent enlistments, the identification of professional test takers and processing “ringers,” improved awareness of the location of applicants, reduction of paper, and better allocation of MEPCOM resources.

JOINT BIOMETRICS OPERATIONAL COORDINATION BOARD (JBOCB) AND JOINT BIOMETRICS TECHNICAL COORDINATION BOARD (JBTCB)

The JBTCB kicked-off in July 2007. The intent of the JBTCB is to support the enterprise operational community through the JBOCB. The JBTCB supports system owners in coordinating change and impact across the biometric enterprise domain as a result of changes driven from the system domain.

Impact: The JBTCB enables horizontal technologies/programs integration among organizations within the Army and across the Services, other government agencies, and industry. The JBTCB provides these biometric communities with opportunities to collaborate and share technical and programmatic information that results in a joint interoperable biometric enterprise system. JBTCB efforts enhance data exchanges among federal departments and agencies.

TRAINING

Training activities focused on improving end user training, simplifying the scheduling process, documenting and validating tasks, and identifying and responding to previously unmet training needs. Through the Biometrics Training Working Level Integrated Product Team (WIPT) and through observation of institutional and operational training, PM Biometrics collected information on training needs. During FY07, participation in the Biometrics Training WIPT increased to more than two dozen organizations within the biometrics community of interest. Both BAT and BISA training teams revised existing training and developed new training materials to better support BAT users and to lay the groundwork for training in support of BISA Tier II. BAT trainers provided Mobile Training Team (MTT) support to more than 40 Army and Marine Corps units in CONUS and at sea, including five weeks of support to the 2nd Brigade, 25th Infantry Division prior to and during its National Training Center (NTC) rotation, as it integrated biometrics into its company-level intelligence support teams. OIF training resources were consolidated under the Director of Operations (Iraq) for PM Biometrics. Working with the Army Learning Management System/Army Distributed Learning System (ALMS/DLS), PM Biometrics developed self-instructional distance learning modules on BAT, BISA, and HIIDE, which are currently in review and scheduled for release in FY08. The Army Space Program Office (ASPO) and PM Biometrics began fielding joint BAT and HIIDE mobile training teams in June 2007. PM Biometrics is working with the

New Systems Training Integration Office (NSTIO) at Fort Huachuca to document and validate biometric tasks and lesson plans in accordance with TRADOC requirements. Working together, ASPO, PM Biometrics, and the Ground Intelligence Support Activity (GISA) developed a single website through which units can request biometric training and obtain information and training materials.

Impact: More Soldiers are receiving realistic, operationally relevant training prior to working with biometric equipment in theater. The process to standardize and document biometric training is underway. Training resources in theater can be deployed flexibly in response to operational needs.

BIOMETRIC IDENTIFICATION SYSTEM FOR ACCESS (BISA)

PM Biometrics awarded a task order for base access operations, maintenance, and support in the CENTCOM Area of Responsibility (AOR) that consolidated efforts being performed under six separate contracts and task orders that were expiring.

BIOMETRIC IDENTIFICATION SYSTEM FOR ACCESS (BISA) & BIOMETRICS AUTOMATED TOOLSET (BAT) BRIDGE DEVELOPMENT

The requirements for the data bridge between BISA and BAT ensure that all BISA enrollments are also passed to BAT. The BISA/BAT Bridge was jointly developed and deployed by PM Biometrics (Language Technology Office and PM Biometrics West Virginia components) and NGIC between May and September 2007.

Impact: This data exchange ensures that BAT has access to the greatest amount of information to facilitate identification of suspected insurgents and enhance biometric data sharing capabilities.

BISA TIER I OPERATIONS

There are 10 Tier I sites in Iraq. These 10 sites were fielded between mid-2005 and May 2006. Tier I provides a turnkey solution (facilities, power, communications, storage, and labor are included) for base access control using a PKI-enabled smart card that allows for authentication of the card and biometric verification that the card-bearer is the individual to whom the card was issued. The Tier I configuration is ideal for areas where there is little or no infrastructure. These 10 sites are preparing to undergo a technology refresh to replace aging equipment and reduce costs.

Impact: At the conclusion of FY07, BISA has issued more than 230,000 smart cards, denied base access to nearly 700 individuals, and has enabled the matching of approximately two dozen latent prints collected from IEDs and exploitation of other sensitive sites.

TIER II DEVELOPMENT

Tier II accomplishes the same function as Tier I, yet does so with a significantly reduced hardware requirement, thus providing a smaller, more mobile version of the BISA system. Funds were made available for the system's development in December 2006. The system was completed in FY07 and is now in the final stages of testing.

Impact: Provides the same level of functionality as Tier I operations in a mobile form-factor.

DAYWORKER

Dayworker is a modification of BISA and is tailored to support the population of workers who are not assigned to a specific contract over a long period of time but who still require access to U.S.-controlled facilities to perform work. The Dayworker system allows for these individuals to be biometrically screened and adjudicated for access. When the individual requires access, he will be identified against the biometric access roster and verified to be in good standing on the basis of a live scan iris match to the stored database. Dayworker was developed during the past year and is currently finishing up laboratory testing and preparing for field operational assessment.

Impact: Ensures that all persons accessing U.S.-controlled facilities are biometrically screened.

DoD INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION PROCESS (DIACAP)

BISA is in the process of completing a "system" security accreditation that will ensure that the system achieves an acceptable risk level and minimizes any security vulnerabilities to be granted an Authority to Operate (ATO) or Interim ATO. BAT is in the process of completing a "type"security accreditation that will ensure that the system achieves an acceptable risk level and minimizes any security vulnerabilities to operate as a Program of Record. NGA is under development and working on the process for accreditation.

Impact: Office of Management and Budget (OMB) requirements for certification and accreditation directly support program and project funding. Accreditation enables greater security for our biometrics system and provides the Warfighter reliable, secure systems in theater.

PLANS OF ACTION AND MILESTONES (POA&M)

BISA POA&M is the tool for identifying tasks that need to be accomplished to remediate any identified vulnerabilities specific to the BISA system. BAT POA&M is the tool for identifying tasks that need to be accomplished to remediate any identified vulnerabilities specific to the BAT system.

Impact: POA&M directly supports a Federal Information Systems Management Act (FISMA) report (which acts as a report card) for each system and is submitted on a quarterly and annual basis to show if the IA posture is acceptable. The POA&M is a performance monitor that shows how much progress is made to meet compliance and is instrumental in the event of audits by Government Accountability Office and/or the Inspector General.

BIOMETRICS AUTOMATED TOOLSET (BAT)

PM Biometrics deployed BAT 4.0 and assumed program management responsibilities for the BAT system from the Army G-2 to include materiel development, ongoing operational support, and integration into the Biometrics FoS. This major systems development effort will continue to be led from Fort Huachuca but with PM oversight and acquisition discipline. PM Biometrics led the staffing of the BAT Transition Plan, which gained 3-star approval from the major BAT stakeholders: Army G-2, Army G-3/5/7, Army TRADOC, and the Assistant Secretary of the Army for Acquisition, Logistics & Technology (ASA(ALT)). The final coordination signature was obtained in August 2007.

Impact: Since its inception, BAT has continued to evolve as an effective, non-lethal weapon system in the Global War on Terrorism by constantly meeting and satisfying new and emerging operational, functional, and technical requirements.

PM CONTRACTING STRATEGY FOR BAT

Along with the transfer of the BAT system, the PM developed a contracting strategy for BAT systems development and integration for the next fiscal year and beyond. The PM has finalized a new task order with the BAT systems development integrator.

Impact: The strategy provides acquisition rigor and development discipline to the BAT program along with continuous support for the BAT in theater.

FIELDING OF BAT VERSION 4.0 SERVICE PACK 5 (V4.0/SP5) & DISCOVERY SYNCHRONIZATION SERVICE (DSS) VERSION 2.7

Upon assuming responsibility for the BAT, PM Biometrics led a phased fielding of the BAT v4.0/SP5 and DSS v2.7. Deployment of DSS v2.7 (Phases 1 and 2) was completed 23 June 2007 with no major issues identified. Deployment of SP5 to all servers (Phases 3 and 4) was completed on 6 July 2007, with a small number of off-network servers updated as they became available based on mission requirements. Deployment of SP5 to all clients (Phase 5) began on 16 July and was completed on 30 September 2007.

Impact: BAT v4.0/SP5 and DSS v2.7 accelerated several key architectural and functional enhancements to the field, which provided an interim solution to answer immediate network and integration issues.

BAT VERSION 5.0

PM Biometrics contracted with a systems integrator to develop the next version of the BAT and Discovery Synchronization Service (DSS) software to sustain current capabilities and meet new user requirements. The systems integrator submitted a draft Functional Requirements Document (FRD) on 31 August 2007. The FRD will be used to validate and prioritize user requirements for the software release through a Systems Requirements Review (SRR) and to develop a project schedule.

Impact: BAT v5.0 will provide several key enhancements based on user requirements that have emerged since the fielding of BAT v4.0.

BAT OPERATIONS & MAINTENANCE

PM Biometrics worked in conjunction with CENTCOM to establish biometric cells in Iraq and Afghanistan. PM Biometrics contracted with a systems integrator to hire and deploy an additional 22 field support engineers to the AOR, along with additional trainers and database administrators for PM Forward. The PM established a PEO EIS e-tracker system as the primary method of asset visibility and lifecycle management of BAT equipment and established an initial level of forward depot support through Ground Intelligence Support Activity (GISA).

Impact: The establishment of biometric cells in Iraq and Afghanistan has provided ongoing support to the Warfighter and dramatically improved theater management of biometrics.

FINANCIAL REPORT

The FY07 Biometrics Task Force (BTF) budget was structured to:

- Synchronize and integrate existing and new technologies throughout DoD
- Provide identity dominance, protection, and management through integrated joint biometric programs
- Establish and maintain an authoritative biometric data source to provide timely, accurate, and comprehensive Identity Superiority to the Warfighter.

The adjacent table depicts the BTF's FY07 appropriated budget, congressional add, and supplemental funding provided to support immediate Warfighter requirements in the Central Command (CENTCOM) area of responsibility (AOR).

FY07 BUDGET

Categories ($000)	OMA	OPA	RDTE
BTF Appropriations Budget	$ 10,332	$ 1,465	$ 16,505
Supplemental Budget	$ 222,300	$ 101,950	$ 59,900
Total	**$ 232,632**	**$ 103,415**	**$ 76,405**

The BTF government staff, augmented with Contract Manpower Equivalents (CMEs), significantly advanced DoD Biometrics Strategy, Policy, Standards, Requirements Validation, and biometric equipment Test and Evaluation goals and provided support to Combatant Commands.

The Joint Requirements Oversight Council (JROC) endorsed the Quick-Look Capabilities Based Assessment (QL-CBA) decision brief on 28 September 2006. The CBA recommendation included funding requirements in FY07 to fulfill critical biometric capability gaps.

The funding was provided in the FY07 supplemental request to address operational needs within the CENTCOM AOR, including base access & security, joint biometrics training, software solutions, and procuring communications equipment.

LIST OF ACRONYMS

ABIS
(DoD) Automated Biometric Identification System

ACO
Access Card Office

AFB
Air Force Base

AFCEA
Armed Forces Communications and Electronics Association

ALMS/DLS
Army Learning Management System/ Distributed Learning System

AOR
Area of Responsibility

API
Application Programming Interface

ASA(ALT)
Assistant Secretary of the Army for Acquisition, Logistics & Technology

ASD(NII)
Assistant Secretary of Defense for Networks and Information Integration

ASPO
Space Program Office (Army)

AT/FP
Anti-terrorism/Force Protection

ATO
Authority to Operate

ATEC
Army Test and Evaluation Command

AUSA
Association of the U.S. Army

BAT
Biometrics Automated Toolset

BCIE
Biometric Collection and Identification Equipment

BDS
Biometrics Data Sharing

BFC
Biometrics Fusion Center

BID
Biometrics Integration Directorate

BISA
Biometric Identification System for Access

BMO
Biometrics Management Office

BOD
Biometrics Operations Directorate

BSWG
DoD Biometric Standards Working Group

BTF
Biometrics Task Force

CAC
common access card

CALL
Center for Army Lessons Learned

CBA
Capabilities Based Assessment

CBT
computer based training

CDD
Capability Development Document

CDS
Cross Domain Solution

CENTCOM
U.S. Central Command

CIO
Chief Information Officer

CITeR
Center for Identification Technology Research

CJIS
Criminal Justice Information Services (FBI)

CJTF
Combined Joint Task Force

CM
configuration management

CME
Contract Manpower Equivalent

COCOM
Combatant Command

COI
Community of Interest

COMSEC
Communication Security

CONUS
Continental United States

COTS
commercial off-the-shelf

CONOPS
concept of operations

CPD
Capabilities Production Document

C&T
Concepts & Technologies

DBEKS
DoD Biometrics Expert Knowledge System

DDB
Director, Defense Biometrics

DDR&E
Director, Defense Research and Engineering

DEERS
Defense Enrollment Eligibility Reporting System

DepSecDef
Deputy Secretary of Defense

DHS
Department of Homeland Security

DIA
Defense Intelligence Agency

DIACAP
DoD Information Assurance Certification and Accreditation Process

DISA
Defense Information Systems Agency

DISR
DoD IT Standards Registry

DITSCAP
Defense Information Technology Security Certification and Accreditation Process

DMDC
Defense Manpower Data Center

DoD
Department of Defense

DoDD
DoD Directive

DOJ
Department of Justice

DOTMLPF
doctrine, organization, training, materiel, leadership, personnel, and facilities

DSS
Discovery Synchronization Service

EA
Executive Agent

EBTS
DoD Electronic Biometric Transmission Specification

EMIO
Expanded Maritime Interception Operations

ERR
Emerging Results Report

EUCOM
U.S. European Command

EXCOM
Executive Committee

FBI
Federal Bureau of Investigation

FISMA
Federal Information Systems Management Act

FoS
Family of Systems

FPED
Force Protection Equipment Demonstration

FPBR
Friendly Personnel Biometrics Repository

FRD
Functional Requirements Document

FY
Fiscal Year

G-2
Army Assistant Chief of Staff, Intelligence

G-3
Army Operations, Plans, & Training

GISA
Ground Intelligence Support Activity

GOTS
government off-the-shelf

GSA
General Services Administration

GWOT
Global War on Terrorism

HIIDE
Handheld Interagency Identity Detection Equipment

HQDA
Headquarters, Department of the Army

IA
Information Assurance

IAFIS
Integrated Automated Fingerprint Identification System

IBIA
International Biometrics Industry Association

IDIQ
Indefinite Delivery Indefinite Quality

IDS
Identity Dominance System

IED
improvised explosive device

IEEE
Institute of Electrical and Electronics Engineers

INCITS
M1 – National Biometrics Standards Body

IPM
Identity Protection and Management

ISAF
International Security Assistance Force (NATO)

ISP
Information Support Plan

IT
information technology

ITL
Information Technology Lab

JBAWG
Joint Biometric Architecture Working Group

JBOCB
Joint Biometrics Operational Coordination Board

JBSESC
Joint Biometrics Senior Executive Steering Committee

JBTCB
Joint Biometrics Technical Coordination Board

JCIDS
Joint Capabilities Integration and Development System

JFCOM
U.S. Joint Forces Command

JFI
Journal of Forensic Identification

JITC
Joint Interoperability Test Command

JMD
joint manning document

JROC
Joint Requirements Oversight Council

JTC 1/SC 37
International Biometric Standards Body

JUONS
Joint Urgent Operational Needs Statement

KM
Knowledge Management

LTO
Language Technology Office

MAGTF
Marine Air-Ground Task Force

MEF
Marine Expeditionary Force

MEPCOM
U.S. Military Entrance Processing Command

MEPS
Military Entrance Processing Station

MET
Military Entrance Testing

MEU
Marine Expeditionary Unit

MISTC
MAGTF Integrated Systems Training Centers

MNC-I
Multinational Corps – Iraq

MNF-I
Multinational Forces – Iraq

MNF-W
Multinational Forces – West

MOS
Military Occupational Specialty

MTT
Mobile Training Team

NaIL
Naval Innovation Laboratory

NATO
North Atlantic Treaty Organization

NCIS
Naval Criminal Investigative Service

NCOW
Net-Centric Operations and Warfare

NCTC
National Counterterrorism Center

NGA
Next Generation ABIS

NGIC
National Ground Intelligence Center (Army)

NIMDOC
Naval Identity Management Development and Operations Capability

NIST
National Institute of Standards and Technology

NIPR
Nonclassified Internet Protocol Router

NPR
National Public Radio

NR–KPP
Net Ready Key Performance Parameter

NSA
National Security Agency

NSF
National Science Foundation

NSTIO
New Systems Training Integration Office

NSTC
National Science and Technology Council

NTC
National Training Center

OASIS
Organization for the Advancement of Structured Information Standards

OCPA
Office of the Chief, Public Affairs

OEF
Operation Enduring Freedom

OIF
Operation Iraqi Freedom

O&M
Operation and Maintenance

OMA
Operations & Maintenance, Army

OMB
Office of Management and Budget

OPA
Other Procurement, Army

OPNAV
Office of the Chief of Naval Operations

OPTEVFOR
Navy Operational Test and Evaluation Forces

OSD
Office of the Secretary of Defense

PEO EIS
Program Executive Office for Enterprise Information Systems

PKI PMO
Public Key Infrastructure Program Management Office

PM
Project Manager

POA&M
Plans of Action and Milestones

PSA
Principal Staff Assistant

R&D
research and development

RAPIDS
Real-time Automated Personnel Identification System

RFI
request for information

RM
resource management

S&T
science and technology

SAG
Stakeholder Advisory Group

SCA WG
Standards & Conformity

Assessment Work Group

SIPR
Secure Internet Protocol Router

SOA
Service Oriented Architecture

SRR
System Requirements Review

SCG
Security Classification Guide

SCSCG
Smart Card Senior Coordinating Group

SDK
Software Development Kit

SOCOM
U.S. Special Operations Command

SOP
standard operating procedure

SP
service pack

SPAWAR
Space and Naval Warfare Systems Command

SSAA
System Security Authorization Agreement

SSE
Sensitive Site Exploitation

T&E
test and evaluation

TBCMS
Tactical Biometric Collection and Matching System

TDA
Table of Distribution and Allowances

TNT
Tactical Network Topology

TRADOC
Training and Doctrine Command (Army)

TTPs
Tactics, Techniques, and Procedures

USACIL
U.S. Army Criminal Investigation Laboratory

USAF
U.S. Air Force

USG
U.S. government

USMC
U.S. Marine Corps

USN
U.S. Navy

VBSS
Vessel Boarding Search and Seizure

VoIP
Voice over Internet Protocol

WIPT
Working Integrated Product Team

XML
eXtensible Markup Language

http://www.biometrics.dod.mil