

# How Does the Military View Biometrics?

*Interim Findings from an  
Elicitation Survey done for the Department of  
Defense Biometrics Management Office*

Department of Defense  
Biometrics Management Office  
<http://www.dod.mil/nii/biometrics>

DEPARTMENT OF DEFENSE



POSITIVE IDENTIFICATION



John Woodward, Deputy Director

## Purpose

- Part I
- Survey Mechanics
- Part II
- Survey Analysis
  - Recommendations by mission areas
  - Categorization
  - General observations

# Survey Announced by Deputy Secretary of Defense



**Deputy Secretary  
of Defense Paul  
Wolfowitz**

12/04/2002 10:18 7036930937 C AND D PAGE 02

 **DEPUTY SECRETARY OF DEFENSE**  
1010 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1010 

**NOV 27 2002**

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS  
UNDER SECRETARY OF DEFENSE (ACQUISITION,  
TECHNOLOGY & LOGISTICS)  
UNDER SECRETARY OF DEFENSE (PERSONNEL & READINESS)  
UNDER SECRETARY OF DEFENSE (POLICY)  
DIRECTOR, DEFENSE RESEARCH & ENGINEERING  
ASSISTANT SECRETARY OF DEFENSE (C3I)  
ASSISTANT SECRETARY OF DEFENSE (HEALTH AFFAIRS)  
ASSISTANT SECRETARY OF DEFENSE (INSTALLATIONS &  
ENVIRONMENT)  
ASSISTANT SECRETARY OF DEFENSE (SOLIC)  
DEPUTY UNDER SECRETARY OF DEFENSE (READINESS)  
DEPUTY UNDER SECRETARY OF DEFENSE (LOGISTICS &  
MATERIAL READINESS)  
PRINCIPAL DEPUTY ASSISTANT SECRETARY OF DEFENSE  
(RESERVE AFFAIRS)

*2002*

**SUBJECT: Biometrics Survey**

The purpose of this memorandum is to announce a biometrics survey and solicit your support. The Department of Defense Biometrics Management Office (BMO) and RAND are conducting a survey of the requirements for biometrics in DoD. Biometrics refers to the automatic recognition of a person using that person's distinguishing traits; examples include digitized fingerprints, hand geometry, iris recognition, speaker (voice) recognition and many others.

The Department of Defense has long supported work in biometrics and the creation of the DoD BMO reflects the growing importance of biometrics for access control, information assurance, and business processes. RAND will schedule an interview with you and members of your staff to determine your short-, mid- and long-range plans for using biometric technologies in your respective mission areas. RAND will also solicit your input on how biometrics is used or could be used best in your mission areas. Prior to the interview, RAND will coordinate with your point of contact and, if you desire, provide a tailored educational briefing to your staff assistants on DoD biometrics and the goals of the survey.

The results of this survey, along with other requirements analysis efforts, will be used by the BMO to determine the department's road ahead for strategically inserting biometric technologies into our mission processes. For your information, attached to this memorandum is a brief tutorial on biometrics and DoD's biometric initiatives.

To schedule the educational briefing and survey interview, please furnish the name, phone number and email address of your point of contact to Ms. Aryn Thomas at RAND. aryn@rand.org, (703) 413-1100, extension: 5530 by December 20, 2002.

*27 Nov 02*

Attachment  
As Stated  U18087-02



# RAND's Survey Methodology

## Convenience Sample

- Total
  - 54 Interviewees
  - 125 Participants

## Advantages

- Detailed, qualitative data
- Flexible, unobtrusive approach

## Interview Protocol

- Semi-structured interview used
  - Read-ahead sent
  - Open-ended questions asked
  - Memorandum sent to BMO

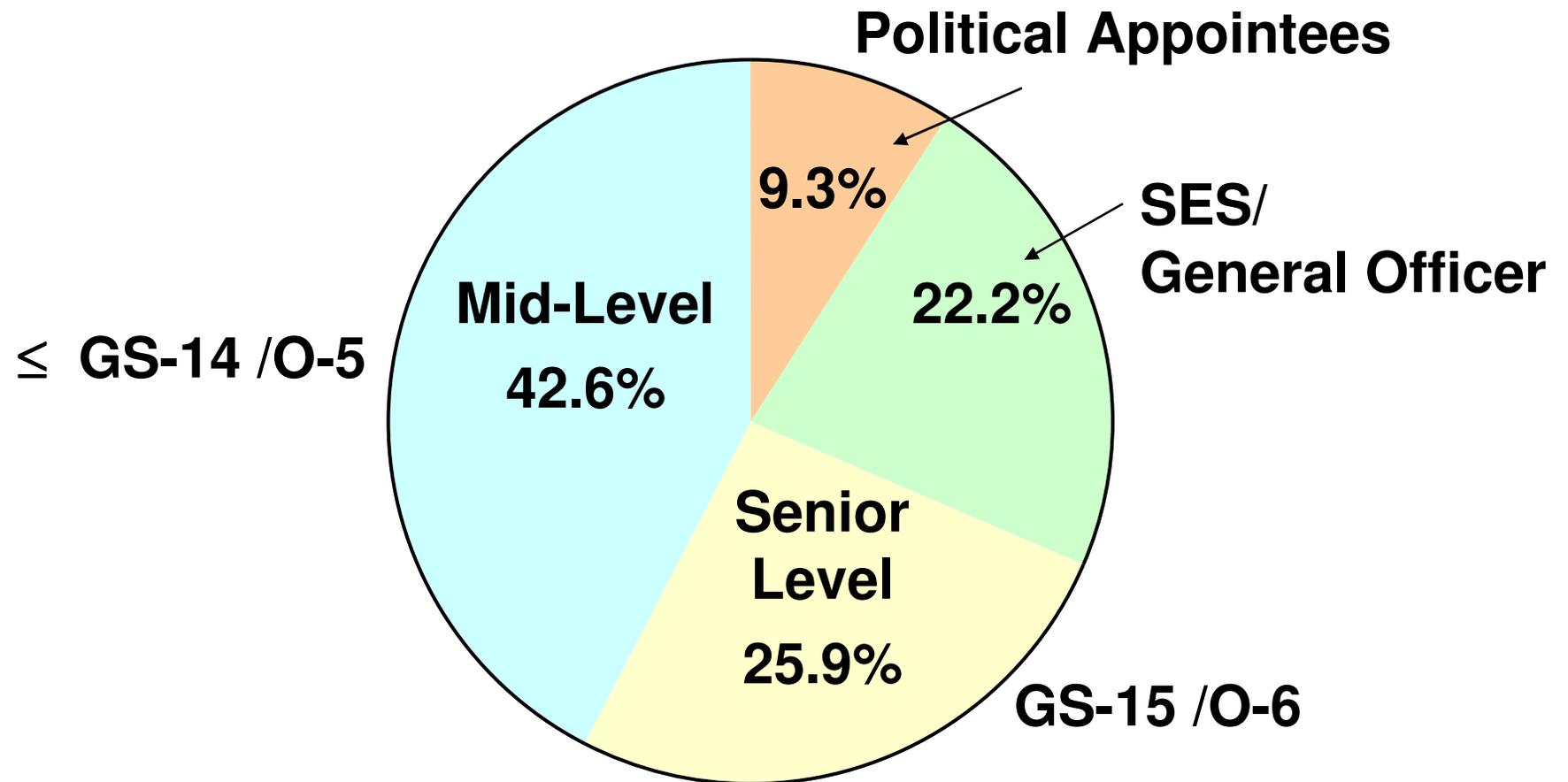
## Disadvantages

- Not a representative sample of DoD

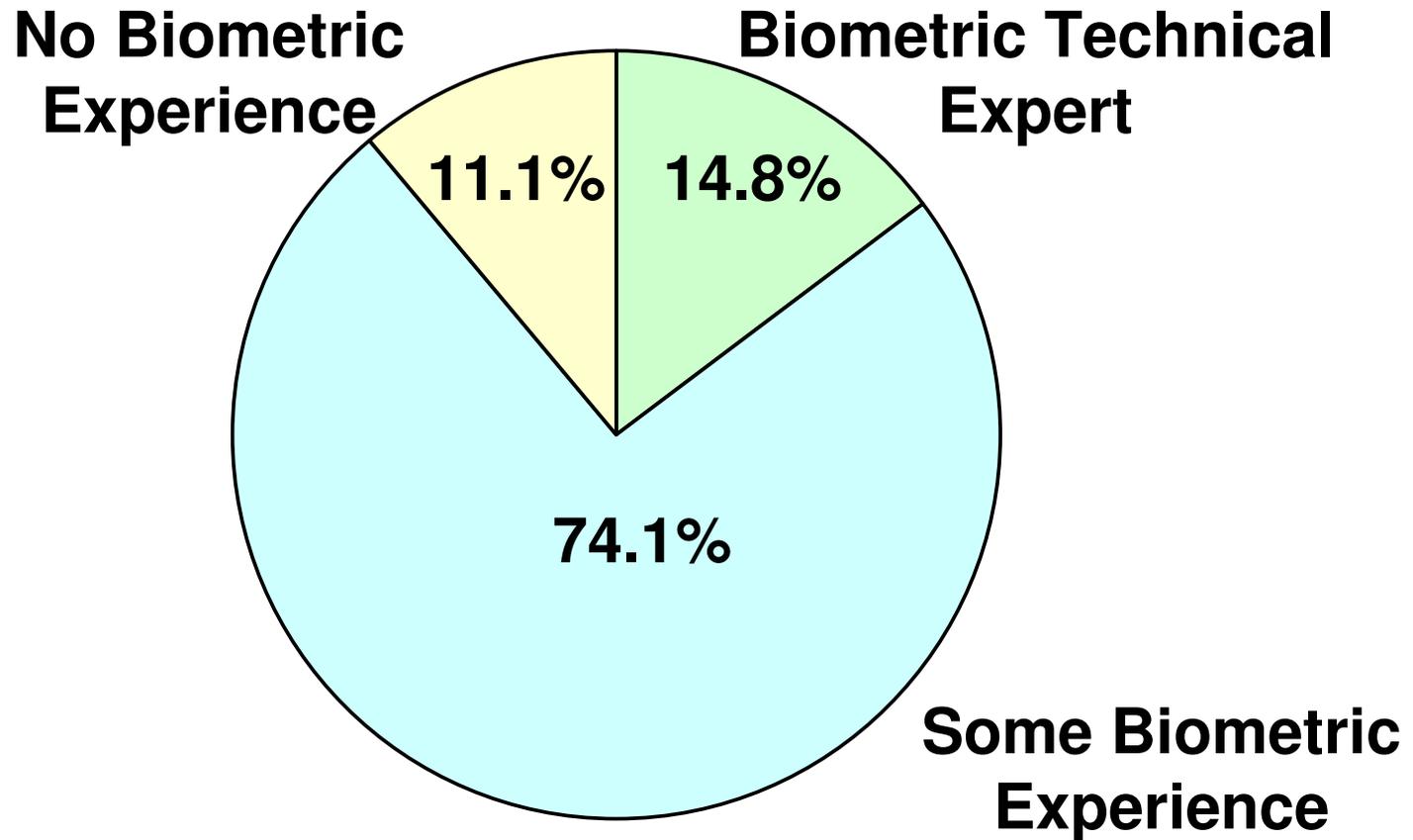
## Major Deliverables

- Survey database
- Documented briefing

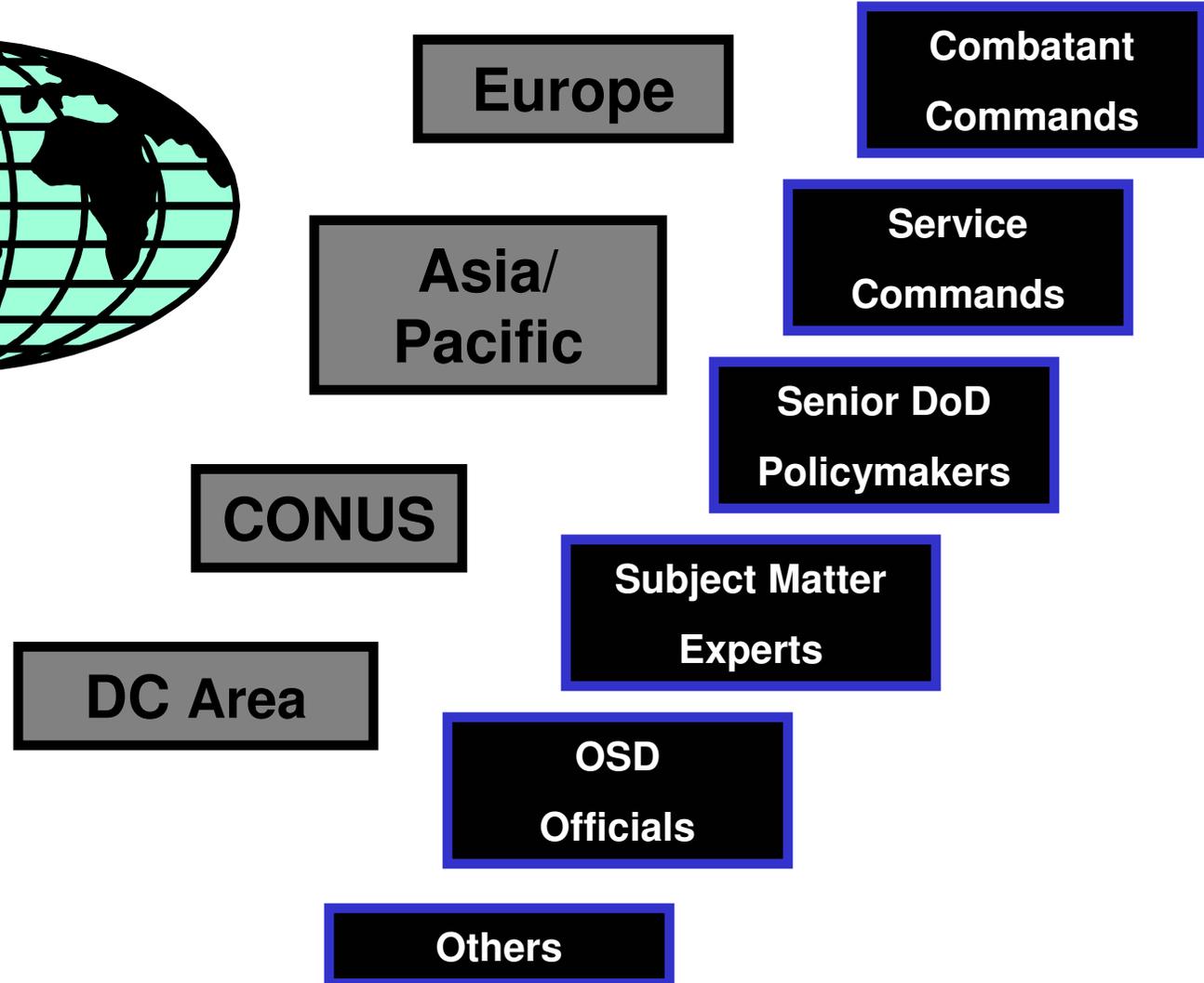
# Position & Affiliation of Interviewees



## Expertise of Interviewees



# Where RAND Interviewed



## **Interviewees' Recommendations for Biometrics—By Mission Area**

- **Physical Access**
- **Biometrics with Common Access Card**
- **Logical Access**
- **Identity Authentication**
- **Processing of Red Force**
- **Tactical--Pro**
- **Tactical--Con**

# The Building Blocks for Biometrics

- **Foundation**
  - **Identity Authentication**
- **Applications**
  - **Logical Access**
  - **Physical Access**
  - **Tactical**
- **Drivers**
  - **Accountability in Business Processes**
  - **Prevention & Deterrence of National Security Threats**
  - **Resource Optimization**

# Foundation: Improve Identity Authentication for DoD

- Currently, it is difficult for DoD to know if a person poses a potential threat or has had past bad dealings with DoD or is using his or her true identity
  - Because DoD does not link identity to a unique characteristic of a person (biometric)
  - Particularly a problem when dealing with terrorists, criminals, & similar threats
- Support for DoD to use biometrics to fix identity of personnel who access DoD facilities

# Application: Improve Physical Access Control

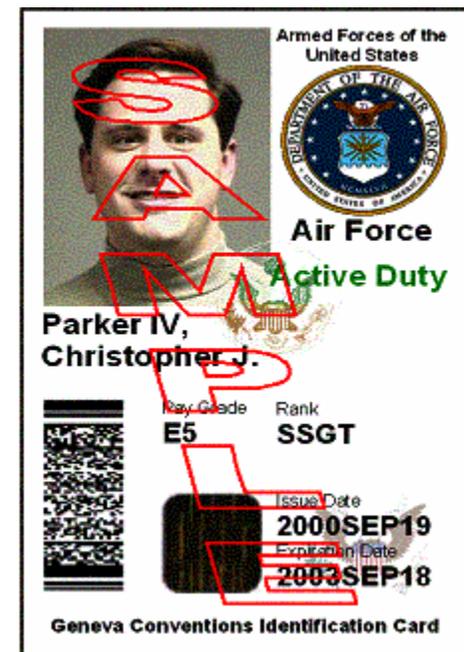
- “Guard at the gate” subject to fatigue, fraud, distraction, inattention, & corruption
- DoD needs biometrics to:
  - Verify in a timely manner the identity of persons seeking access to DoD installations, facilities, & physical space
  - Enhance force protection measures
  - Link identity to an inherent part of a person
  - Have a robust audit trail of persons accessing certain physical spaces

# Application: Improve Logical Access Control

- Current system has pitfalls:
  - Security
    - Passwords are easily compromised, shared
    - Passwords do not create robust audit trails
  - Administration
    - Costs of password maintenance for DoD
    - Costs of inconvenience for user
- DoD needs biometrics to augment or replace passwords:
  - Increased security
  - Increased convenience
  - Better audit trail

## Application: Biometrics & Common Access Card

- Strong support for biometrically enabled CAC
- CAC is already in place and established by DoD policy
- Biometrically enabled CAC is seen as
  - Promoting DoD interoperability by leveraging a common platform
  - Augmenting local commander's access control measures



# Application: Improve Tactical Capabilities for the Warfighter

- Biometrics in tactical environment is a technical and operational challenge
- Interviewees identified the following tactical areas for biometrics:
  - Securing select tactical information systems
  - Blue force processing of red force data
    - EPWs, detainees
    - Others
    - Need for this data to be shared with USG agencies

# Driver: Optimize Use of DoD's Resources

- Post 09/11, DoD's overall force protection posture is very resource intensive
  - Manpower
  - Money
  - Current posture not sustainable for long-term
- Short-term, high-priority exists to use technology to provide security & reduce resources
- Strong support for using biometrics to meet this challenge

## Driver: Improve Detection & Deterrence of National Security Threats

- DoD currently collects ten fingerprints from military members, civil servants, & others
- DoD has this biometric information stored but underutilizes this database
- DoD should use this biometric database as an aid for:
  - Counterterrorism
  - Counterintelligence
  - Criminal investigations
- DoD should collect biometrics from certain persons who access DoD installations
- Strong support from military intelligence & law enforcement communities
- Concerns raised about policy & privacy issues

## Driver: Improve Accountability for DoD Business Processes

- DoD suffers fraud in various entitlement programs, etc.
- DoD needs credible deterrence to prevent thefts
- Support for using biometrics in business processes to create fixed identity to defeat use of alias as well as a robust audit trail

# Interviewees' General Observations on Biometrics

## Support

- **Nearly all are positive about biometrics & expect to see it deployed in various DoD applications**
- **Nearly all welcome any technology (biometrics) that can help DoD in force protection**
- **Strong support for a biometrically enabled CAC as a short-term priority**
- **Strong support for DoD to use biometrics to perform better physical & logical access control**
- **Support to use biometrics for auditing & tracking, identification of national security threats, business processes, etc.**

# Interviewees' General Observations about Biometrics (cont'd)

## Concerns

- **How much does it cost the end-user to implement, support, & maintain biometrics?**
- **How well do the various biometrics perform?**
- **How robust is the technology in different environmental conditions?**
- **How does the use of biometrics affect processing times (throughput)?**
- **How will policy issues, like privacy, be addressed?**

## Summary

- **Survey reports data from 54 interviewees, a broad cross section of DoD**
- **Broad support for biometrics in DoD's future**
- **Support for using biometrics in several mission areas**
- **Issues remain in policy, operational, & technical realms**