A. Panel Statement

a. Title of Panel**: Department of Defense (DoD) Wide Information Assurance Program (DIAP): Current Initiatives**

b. Panel Chair: **Captain J. Katharine Burton, USN,**
Staff Director, Defense-Wide Information Assurance Program
Office of the Assistant Secretary of Defense for Command, Control,
Communications, Intelligence (C3I), Infrastructure and Information
Assurance Directorate

c. Panelists: Terry Bartlett, IA Readiness Functional Area, DIAP
George Bieber, IA Program Management Office, D25, DISA
Jim Christy, Law Enforcement/Counter-Intelligence Liaison, DIAP

d. Session abstract:

With the maturing of the DoD's Information Assurance programs, a number of initiatives are having significant impact on how the Department is addressing the various areas of Information Assurance. As a result, some of the more difficult areas to address are being investigated, solutions proposed and the groundwork laid to change policies, processes and management in these areas. This panel will begin with an overview of where the DIAP stands today and what activities/initiatives have been accomplished in the past year. Following that will be 10-15 minutes presentations on three areas where significant effort is currently being spent: IA Metrics, IT/IA Professionalization and Law Enforcement. Each presenter will discuss where that initiative currently stands, what activities are going on within DoD and the various services/agencies, and what the activity will contribute to the improvement of the IA posture of the Department. Although these activities are specific to the DoD, similar/related efforts exist throughout the Federal government, as well as commercial and private sectors.   In fact, some of the activities have benefited directly from these related efforts. The panel will discuss how some of the solutions from other areas have had to be adapted to the DoD environment, and where some unique solutions have been developed – which may have benefit to other activities. Following the presentations, there will be an opportunity for the audience to ask questions of the panel members.

e. Brief summary of panelist's topics:

(1) IA Metrics: **To provide some accurate and defendable way to measure progress (or lack thereof) in the Information Assurance arena, metrics are needed. Unfortunately, many of the numbers used in IA neither measure anything useful (therefore providing little insight into the state of the activity), nor can be supported under investigation.   Additionally, too much of what is happening in the IA arena is not measured at all.   The DIAP**

effort is focussed on developing a framework for DoD IA metrics that makes sense within the DoD context. With that framework, we can then develop, adapt or incorporate metrics that have been developed in other related areas to provide a relatively complete and accurate picture at a point in time of the DoD's IA posture. This effort is also trying to take advantage of work that other activities are doing in this arena, as well as sharing the DoD's experience in developing appropriate metrics.

(2) IT/IA Professionalization Management Within DoD: **Two issues have resulted in a professionalization effort within DoD: (1) the need to recruit and retain qualified professional s in an extremely competitive environment and (2) the need to develop a career path with appropriate training and opportunities for individuals in a growing new area. The DoD chartered an Integrated Process Team (IPT) in 1998 to look at what the Department needed to do to begin identifying who was in the IA/IT community, what training/education was required and what policy changes were needed. This was not the initial effort the department had made in this area, but was the most comprehensive effort to date. Related to this, or as a result of this IPT, the services and agencies have made significant strides in professionalizing the workforce. This presentation will discuss some of those professionalization efforts.**

(3) Law Enforcement's role in Supporting Information Assurance: **Many communities that have not traditionally worked together are now finding that they must cooperate in order to ensure accomplishment of the IA mission. In particular, the Law Enforcement community has become essential to the enforcement arena of Information Assurance. To ensure proper investigations which then lead to prosecution of computer-related crime, roles and responsibilities – "lanes in the road" – need to be well understood and followed. This presentation will discuss the new DoD Computer Forensics Lab, Defense Computer Investigations Training program and the DoD Computer Crime Workshop, hosted by the DIAP in May 2000.**

f. Background of Audience: **Technical and non-technical, primarily management responsible for IA programs for their organization – anyone who has an interest in the individual presentation areas would be welcome**.

BIOS

CAPTAIN J. Katharine Burton, USN, Staff Director, Defense-Wide Information Assurance Program

Captain J. Katharine Burton, a native of Oklahoma City, OK, graduated from the University of Oklahoma (OU) in May 1976 with a Bachelor of Arts Degree in English Literature. Captain Burton is a 1998 graduate of the National War College where she received a Master of Science Degree in National Security Strategy with a certificate from the Information Strategies Concentration Program. She also holds a Master of Arts Degree in Management Information Systems from George Washington University and is a 1986 graduate of the Armed Forces Staff College. Captain Burton served in a variety of tours including command of the Naval Computer and Telecommunications Station (NCTS), Roosevelt Roads, PR,. She currently serves as the Staff Director, Defense-Wide Information Assurance Program (DIAP), in the Information Assurance Directorate of the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (OASD/C3I).

George Bieber, IAPMO, D25, Defense Information Systems Agency

Mr. Bieber is the Chief, Information Assurance (IA) Education, Training, Awareness (ETA) and Products, IA Program Management Office, Defense Information Systems Agency. He provides overall guidance, and is responsible for managing the development, production and dissemination of Department of Defense (DOD) level IA training and awareness. This includes both classroom courseware and award winning distributive CD-ROMs for use by DOD military schools, by individual organization training and awareness programs and by the DOD IA personnel certification program. Previously, Mr. Bieber was an operations research analyst and program manager with the Defense Evaluation Support Activity where he planned, and conducted evaluations of joint communications tests, and exercise of operational concepts. Prior to entering government service, he was an analyst for a number of Defense contractors. Mr. Bieber serves on the Executive Board of the Federal Information System Security Educators Association (FISSEA). He has a Bachelors Degree in History and a Masters Degree in International Studies, with a concentration in computer applications and quantitative techniques.

Terry Bartlett, Information Assurance Readiness Functional Area, DIAP

As a member of the DIAP Staff, Terry serves as the DIAP's Readiness Assessment Team Leader. He is employed currently by Science Applications International Corporation as a Senior Information Assurance Analyst. Terry is a Certified Information Systems Security Professional (CISSP) with substantial background in information technology, military command and control, and project management. He is retired from the US Air Force, has performed in many managerial and staff roles in both military and civilian environments, and has a variety of experience in supervisory, project management, security, auditing, and technical roles. Terry has a Bachelors Degree in Business Administration and a Master of Science Degree in Systems Management.

JAMES V. CHRISTY II, Defense-Wide Information Assurance Program, (DIAP)

Supervisory Special Agent James V. Christy, II is currently detailed from the Air Force Office of Special Investigations, Andrews Air Force Base, MD to the Defense-wide Information Assurance Program, Assistant Secretary of Defense for Command, Control Communications and Intelligence (ASDC3I) as the Law Enforcement & Counterintelligence Coordinator. SA Christy served as the DoD Representative to the President's Infrastructure Protection Task Force (IPTF) from Sep 96 – May 98. The President signed Executive Order, 13010 on 15 Jul 96, creating the Infrastructure Protection Task Force to protect the Nation's critical infrastructure from both physical and cyber attacks. Prior to the IPTF, Jim was detailed to Senator Sam Nunn's staff on the Senate, Permanent Subcommittee on Investigations as a Congressional Fellow, Jan - Aug 96. Senator Nunn specifically requested Jim's assistance for the Subcommittee to prepare for hearings in May - Jul 1996, on the vulnerability and the threat to National Information Infrastructure from computer intrusions. Jim was selected by AFOSI in 1986 as the Assistant Program Manager of Computer Crime Investigations. He was selected as the Director of Computer Crime Investigations, and Information Warfare, in 1989. Jim had the responsibility for management of a special cadre of 69 hybrid special agents and computer specialists. Under Jim's leadership, AFOSI established the first computer forensic lab in DOD which is being benchmarked by many federal, state, and allied law enforcement agencies and is now the Executive Agency responsible for the DoD Computer Forensic Lab. Jim obtained some notoriety as the original case agent in the "Hanover Hacker" case. This case involved a group of German hackers who electronically penetrated DOD computer systems all over the world and sold the information to the Soviet KGB. The case was detailed in the best seller, "The Cuckoo's Egg", by Dr. Cliff Stoll.