PLATFORM INFORMATION TECHNOLOGY DEFINITIONS FOR THE DEPARTMENT OF THE NAVY

27 Nov 07

I. PURPOSE

This document defines Platform Information Technology (IT) for IT networks, systems and IT components within the Department of the Navy (DON). It is based primarily on Department of Defense (DoD) Instruction 8500.1 and Secretary of the Navy (SECNAV) Instruction SECNAVINST 5239.3A. Definitions, concepts and interpretation are derived from these sources.

II. DEFINITION OF TERMS

This section lists terms and definitions that pertain to Platform IT.

GENERAL PURPOSE

A system used for routine administrative and business applications, including payroll, finance, logistics, and personnel management applications. General purpose systems are normally not built for a unique application, and do not fall outside the definition of special purpose systems as defined by DoD 8500 series guidance.

GLOBAL INFORMATION GRID (GIG)

The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to war fighters, policy makers, and support personnel. Includes but is not limited to NIPR, SIPR, JWICS, and NMCI. (Ref: DoDD 8100.1, 19 Sep 2002)

PLATFORM

A vehicle, structure or person that performs a mission in support of US National Security policy; and aboard or in which a DoD national security system may be installed to support assigned missions. Generally, the term "platform" includes, but is not limited to, Aircraft, Ship, Submarine, Shore Facility (such as NOC, JIC, Command Center, Hospital, Base Power Plants), Ground Vehicle (such as HMMWVs, Tanks, Strykers), Remotely Operated Vehicle (such as UAV, USV, UUV), and a Sailor or Marine in the field.

PLATFORM IT

Derived from DoDD 8500.1, Paragraph E2.1.16.4, Platform IT:

1. REFERS TO computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special-purpose systems. PIT does not include general purpose systems.

2. MAY:
   a. Reside aboard or on a platform
   b. Be stand-alone
   c. Have an interconnection to other Platform IT (known as a "Platform IT-to-Platform IT Interconnection")
   d. Have a Platform IT Interconnection (see DoDI 8500.1) to other IT that is not Platform IT (e.g., a general-use ship's network, such as ISNS, or a non-Platform IT system)

BOUNDARY

The physical and/or logical limit of a platform or the physical and/or logical limit of the information system as determined by the system description.

CONNECTION

The physical or logical interface that allows data to flow between components in a system, between systems within a system-of-systems, or between information systems installed onboard different platforms.

1. Platform IT Interconnection (PITI):
   a. A physical or logical connection at or crossing the boundary between a Platform IT system and a non-Platform IT system

2. Platform IT to Platform IT Interconnection (PTPI):
   a. A physical or logical connection at or crossing the boundary between a Platform IT system and another Platform IT system

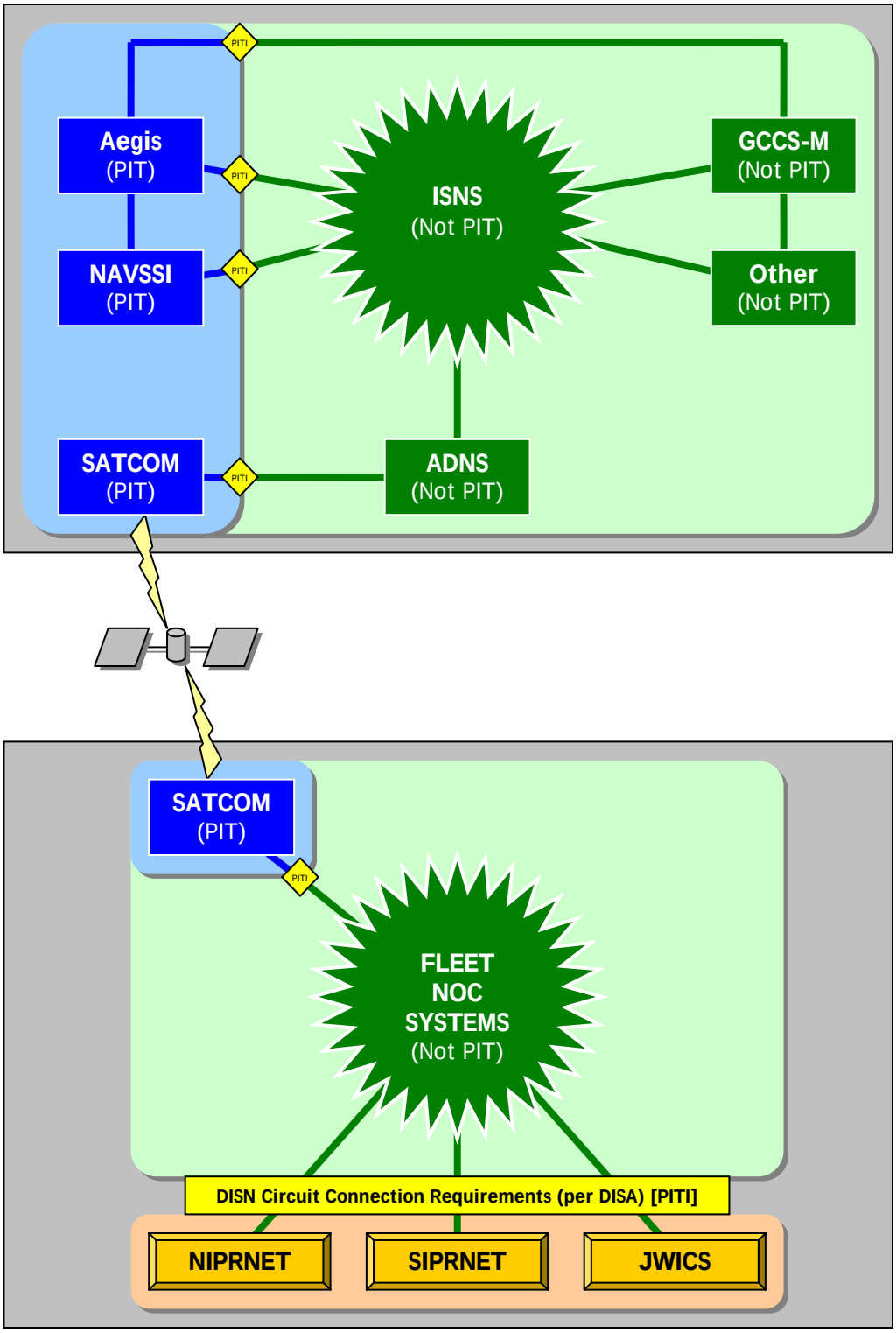

Figure 1 Notional Platform IT Interconnection (Fleet)

Figure 1 shows a notional diagram of interconnection involving Platform IT (blue), Platform IT Interconnection (yellow), non-Platform (green) and the GiG (gold).

REAL-TIME

Systems in which the correctness of the system depends not only on the logical result of computations, but also on the time at which the results are produced or the sense of urgency of the systems information processing and the information processed by the system to completion of the platform's mission.

SPECIAL-PURPOSE SYSTEM

Derived from DoDD 8500.1, Paragraph E2.1.16.4.

System or platform that employs computing resources (i.e., hardware, firmware, and optionally software) that are physically embedded in, dedicated to, or necessary in real time for the performance of the system's mission. Examples of special purpose systems include weapons systems, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems, such as water and electric.

III. BACKGROUND

IA policy applies generally to all IT systems

PROGRAM MANAGERS (PM) are responsible for ensuring sufficient IA is incorporated into their systems whether or not the C&A process is required. Even under a designation of Platform IT, Program Managers must implement the maximum amount of IA consistent with the special-purpose mission performed by the Platform IT.

Per SECNAVINST 5239.3A and Defense Acquisition Policy (the DoD 5000 series, DoN 5000.2, and DoDI 8580.1), IA is applicable to all DoN-owned or -controlled information systems that receive, process, store, display or transmit DoD information, regardless of Mission Assurance Category (MAC), classification or sensitivity.

Both SECNAV and Defense Acquisition Policy are satisfied by employing the tenets of defense-in-depth for layering IA solutions within a given IT asset and among assets; and ensuring appropriate robustness of the solution, as determined by the relative strength of the mechanism and the confidence that it is implemented and will perform as intended. The IA solutions that provide availability, integrity, and confidentiality also provide authentication and non-repudiation.

The goal of IA for DoD/DoN IT systems, as stated in DoD 8500.1, paragraph 4.2, is:

> *"All DoD information systems shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflect a balance among the importance and sensitivity of the information and information assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; the impact of impairment or destruction to the DoD information system; and cost effectiveness."*

The IA Controls provided in DoD 8500.2 apply to the definition, configuration, operation, interconnection, and disposal of DoD information systems. They form a management framework for the Clarification of Platform IT for Navy Information Systems allocation, monitoring, and regulation of IA resources that is consistent with Federal guidance provided in OMB Circular A-130.

The C&A process applies generally to all IT systems, except Platform IT

Per DoDD 8500.1, the C&A process (DITSCAP or DIACAP) is applicable to all DoN-owned or controlled information systems that receive, process, store, display or transmit DoD information, regardless of MAC, classification or sensitivity, except, per DoDD 8500.1 Paragraph 2.3, IT that is considered Platform IT.

Figure 2 shows applicability of the C&A process and IA policy to a situation involving both Platform IT and a Platform IT Interconnection.

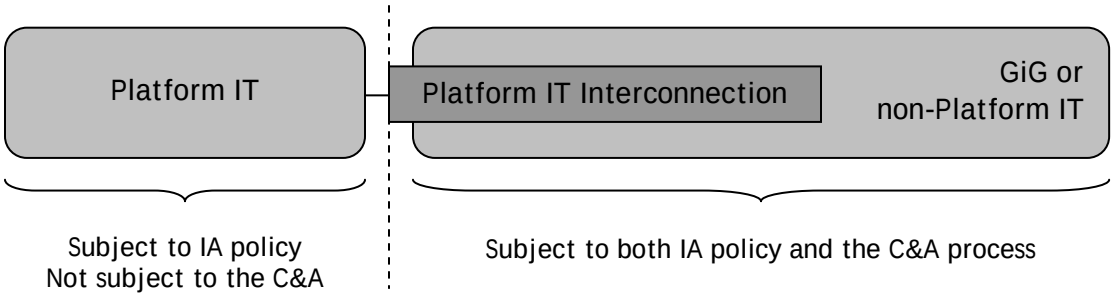

Figure 2 Platform IT

As illustrated in Figure 2, generally all IT is subject to IA policy and the C&A process, but Platform IT is excluded from the C&A process. The Platform IT Interconnection is specifically subject to the C&A process, per DoDD 8500.1.

Special Note about Stand Alone Systems

Per DoDD 8500.1, a stand-alone system (e.g., does not have one or more network connections) is subject to the C&A process unless it meets the definition of Platform IT. An IT system or IT component cannot be classified as Platform IT simply because it is stand-alone.