1. ROLES AND RESPONSIBILITIES

The Office of the Chief Information Officer (OCIO) at major cabinet-level departments is a critical transformation entity in the Federal government. The Chief Information Officer (CIO) position was established by the Clinger-Cohen Act of 1996 as the key factor in helping to align agency investments in information technology (IT) closely with agency mission goals and objectives. In particular, Congress envisioned an executive level leader who would be a member of the agency's top-level management team and who would be able to help translate business needs into IT investments.

This mandate has been further codified by the Office of Management and Budget (OMB) in OMB Circular A-130, which outlines in detail the processes that an agency must implement to fulfill the requirements of the Clinger-Cohen Act. This includes the establishment of an agency-wide Enterprise Architecture to describe the future state of the agency's IT environment that closely aligns technology with the agency's mission. In addition, CIOs are required to implement an agency-wide, mission-focused Capital Planning and Investment Control (CPIC) process, implement adequate IT security for systems and applications; and implement a Records Management process to ensure the effective capture, preservation, management, and disposal of electronic records. Figure 1-1 depicts the expanse of the competency areas that the CIO position covers.

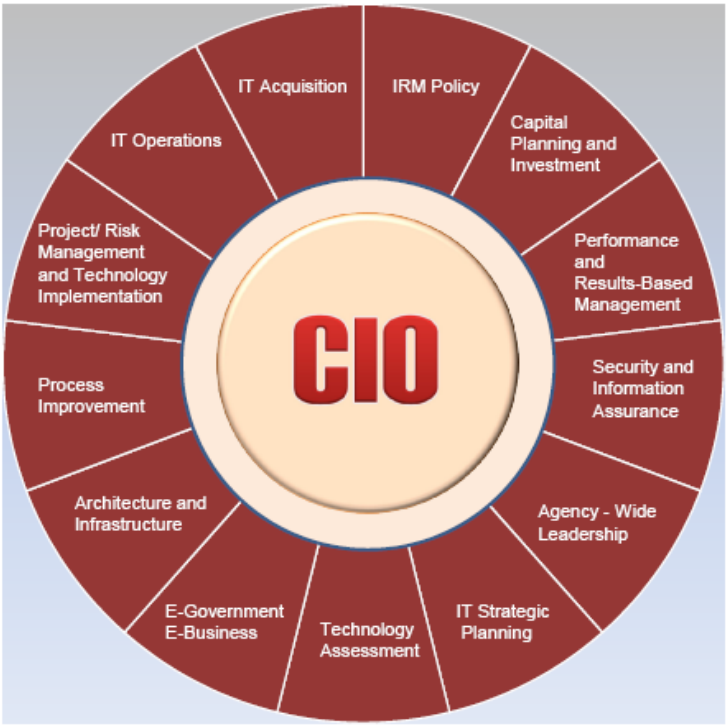

Figure 1-1: CIO Competency Areas

Within the Department of Justice (DOJ), the importance of the mission and the focus on effective information sharing and management emphasizes the important role of the OCIO. This has escalated since September 11, 2001 with the mandate from the Congress and various Executive Orders from the President requiring improved and enhanced information sharing between key Federal agencies, between Federal agencies and State and Local law enforcement and judicial agencies, and between the United States and foreign governments. The application of IT is essential to meet these goals and to ensure the security of U.S. citizens worldwide.

As depicted in Figure 1-2, the DOJ CIO also serves as both a leader and a coordination entity between the Justice Department and other key Federal agencies. This includes the Department of Homeland Security (DHS) and the Director of National Intelligence (DNI), but also State, Local, and Tribal (SLT) governments who have on-the-ground responsibilities for law enforcement, judicial processes, incarceration and first response in the event of a terrorist attack. Because of the importance of the central role in facilitating information sharing among these key entities, interoperable and integrated technology is needed to support these mission processes. To accomplish this, the DOJ CIO needs to lead the effort to both standardize and consolidate key infrastructure to allow intra-agency and cross-agency sharing of data, information and applications and to leverage the use of existing, and the creation of new, enterprise solutions that will improve mission results.

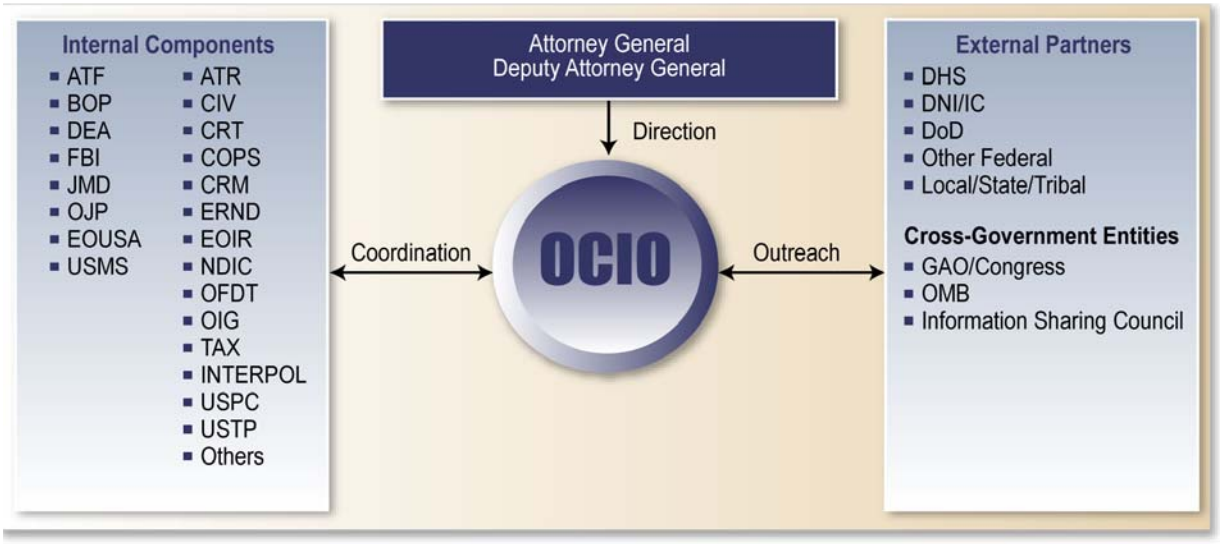

Figure 1-2: DOJ OCIO Key Relationships

To be successful at these broad and complex responsibilities, the DOJ CIO also provides leadership and coordination among the various Components within the Department, each of which has its own critical missions and responsibilities. In many cases the missions are unique to the Component and require specific solutions. The Component CIOs focus on meeting their respective mission IT requirements and providing high quality service to their business customers. However, in many other cases such as IT infrastructure, office automation, case management, administrative support systems, data and information sharing, and records management, there is a need for standardization, consolidation, and sharing of both infrastructure and solutions across the Department. The DOJ CIO provides leadership in facilitating the success of these initiatives by driving synergies and providing cross-cutting capabilities.