

Section F: Information Technology

Introduction

Drug intelligence analysts must be supported by effective, secure, and powerful information systems. The drug intelligence centers and activities require an architecture that permits rapid access by authorized analysts to all relevant information sources; quick information retrieval and sorting; secure information transfer among organizations; and tools to manipulate and analyze the information. Existing information technology and communications systems in the law enforcement community require large-scale improvements in secure interconnectivity. FY 2000 resource levels are not programmed to accommodate these initiatives.

The state of systems architectures today is much improved over that of August 1992, when the *National Drug Control Information Resource Management Plan* was published under Office of National Drug Control Policy (ONDCP) auspices. The Intelligence Community has achieved significant advancements that address many of the requirements for interagency information sharing in the national security realm. For example, secure Internet-type technology has been implemented in the Top Secret environment. The law enforcement community has completed numerous improvements in overall automation across the Federal, state, and local levels. Notable examples of improved automation include DRUG-X, the Drug Enforcement Administration's (DEA) Firebird and Merlin systems, and the National Drug Pointer Index (NDPIX). There are also several positive information-handling and -sharing initiatives involving law enforcement, the Intelligence Community, military components, and regional organizations. Some examples are the Department of Defense-sponsored interagency Anti-Drug Network (ADNET), and the Department of Justice-administered Regional Information Sharing System Network (RISSNET).

Despite these successes, no single organization's system can provide electronic access to all of the drug law enforcement information that is available to support ongoing investigations and analyses. The frequent inability of the various law enforcement and Intelligence Community agencies to share the appropriate data in an expeditious manner, or at all, is still a critical shortcoming.

The key concepts underlying the systems architecture plan defined in this section are the following:

- (1) No agency or level of government has all the drug intelligence available;
- (2) Information sharing is critical to ensuring success—there must be a level of information sharing across all political boundaries (including international, national/Federal, regional, state, and local government entities) and within all

security levels (including Top Secret, Secret, Sensitive But Unclassified, and purely Unclassified);

- (3) Security is a mandatory precursor to information sharing;
- (4) The legal and policy barriers to effective information sharing must be clearly identified, and accommodated or eliminated, where appropriate, to enable technology to help solve the intelligence problems;
- (5) The technical capabilities required begin with electronic mail within and among agencies and analysts, at a minimum, and progress through limited database access and document publishing, and culminate with real-time collaboration, eliminating geographic barriers by using audio, video, and direct access to databases under strictly controlled circumstances; and,
- (6) The key technical connections across the drug intelligence community to provide for information exchange can be improved using current technologies—no further research or development is necessary to implement the initial architecture.

Traditionally, drug intelligence and law enforcement organizations at all levels have developed information systems to meet their own specific requirements, resulting in a proliferation of information systems that are essentially “stovepipes.” Major drug intelligence centers, in particular the National Drug Intelligence Center (NDIC), have very limited access to law enforcement data. The counterdrug community can maximize the efficiency of the intelligence process by adopting a systems architecture that places the relevant information into a series of interoperable “accessible information spaces,” with respect for need-to-know and proper authorization to access information. The creation of shared information spaces will make community-wide electronic access a reality, providing analysts the flexibility to interact with, and gather information from, other organizations. It will also provide the technical foundation for the timely and secure dissemination of intelligence to appropriate customers.

This systems architecture will provide a mechanism for appropriate state and local personnel to interact electronically with one another and their Federal law enforcement counterparts in a secure environment. The goal is to enable all of the drug intelligence analysts with the appropriate credentials to obtain all of the information they need to do their jobs. There is no intent to enable, nor will the system permit, personnel without appropriate clearances to access national security databases, or Intelligence Community analysts to directly access domestic criminal investigative data.

Advances in communications technology have removed most of the technical barriers to information sharing, while also improving methods of protecting information. Technical security measures such as encryption, smart cards, public-private key infrastructures, Internet protocol security standards, biometrics, and firewalls can be used to prevent unauthorized access, allowing network administrators and security professionals to

enforce the standards of need-to-know. The technical means exist for the drug intelligence community to share information securely, but the connecting hardware and software must be widely available throughout participating agencies. Departmental and agency procedures should be reviewed to ensure that they facilitate secure information sharing.

This Plan envisions a future systems architecture that is both secure enough to support information sharing and easily accessible from across the drug intelligence community. The goal is to ensure that all drug intelligence and law enforcement personnel can obtain expeditiously all of the information they have been cleared to receive and need to know. It promotes the use of existing networks and secure Web technology to connect the drug intelligence community. The technical components include more robust, timely, and accurate input into agency databases; adherence to strict security with audit trails; proactive dissemination of non-case-specific law enforcement information to the broader drug intelligence community; single-workstation access to multiple sources of law enforcement and intelligence information; and funding for adequate technical support, life-cycle enhancements, training, user support, and analytic tools.

This section provides 10 specific action items that will create the basis for an effective drug intelligence systems architecture.

F-1. Establish a Systems Policy Review Group (SPRG): To ensure that broad systems standards are developed to guide law enforcement and intelligence agencies, the Counterdrug Intelligence Coordinating Group (CDICG) will establish an SPRG to advise it and help the participating departments and agencies in accomplishing the six initial goals:

- (1) Develop common criteria and define architectural and data standards for drug information-sharing systems focusing on the counterdrug Intelligence Community, the El Paso Intelligence Center (EPIC), the Financial Crimes Enforcement Network (FinCEN), and NDIC;
- (2) Ensure consistency with laws and policies concerning privacy and civil liberties. Information sharing will follow the security, privacy, and technological standards determined for the Global Justice Information Network (Global). The CDICG, based on the recommendations of the SPRG, will consider the advantages of any new data access and transfer initiatives, and the possible legal and policy reasons not to undertake particular proposed initiatives;
- (3) Facilitate electronic connectivity among Federal drug law enforcement personnel;
- (4) Facilitate electronic connectivity among regional, state, and local drug law enforcement personnel;
- (5) Address the policy concerns limiting connectivity between Federal and regional, state, and local personnel; and,

(6) Support agency initiatives to automate case files at an accelerated rate.

F-2. Use Existing Information to Create a Detailed Schedule for Implementing the Drug Law Enforcement Intelligence Architecture: The SPRG, working with the Counterdrug Intelligence Executive Secretariat (CDX) and other experts, will expedite the development of an initial architecture plan and a detailed schedule for its implementation. Concurrent with the SPRG architecture effort, the participating Departments and agencies should begin to plan and budget for the technology enhancements defined in the Action Items listed below. The development of the architecture will take advantage of recent Justice Department studies, the plans for the Intelligence Community Collaborative Operations Network, the creation of the Global Justice Information Network (Global), the Defense Department's Global Information Grid, and other ongoing initiatives in this area.

The planning effort will also take advantage of the conceptual model for information technology architecture (ITA) created under the auspices of the Chief Information Officer (CIO) Council of the Federal Government. The Council has created a common set of terminology and definitions that are appropriate for the drug intelligence information technology architecture effort. The CDICG will ensure that the CIOs are cognizant of the ongoing efforts of the SPRG.

At a minimum, the plan must take the following factors into consideration:

- (1) Information requirements and capabilities—this includes determining which organizations require the various types of information and identifying which organizations have that information available;
- (2) Barriers to information sharing—this includes identifying and seeking resolution to impediments to secure information sharing at the international, Federal, regional, state, and local levels; and,
- (3) Candidates for interconnection at the same level of security:
 - (a) Top Secret—future efforts within the Intelligence Community to augment the existing Intelink;
 - (b) Secret—FBINET, EPIC Internal System, and the NDIC internal network with the ADNET (DEA Merlin already connects);
 - (c) Sensitive But Unclassified—Treasury Enforcement Communications System (TECS), DEA Firebird, U.S. Coast Guard Law Enforcement Information System (LEIS), RISSNET, and certain systems on National Law Enforcement Telecommunications System (NLETS);

- (d) Unclassified—High Intensity Drug Trafficking Area (HIDTA) Information Systems Network (ISN) and other secure and non-secure systems operating on the Internet; and,
- (e) Alternatives for connecting systems that operate at different security levels—the Counternarcotics Command Management System (CNCMS) and the Federal Bureau of Investigation (FBI) currently operate systems with limited connectivity between Unclassified and Secret systems. The technology, policies, and procedures that enable this type of connectivity will be examined for broader application.

F-3. Extend Secure Connectivity Among Federal Drug Intelligence Personnel: It is critical that the drug intelligence personnel at all Federal law enforcement agencies and centers have the ability to contact and collaborate securely with their counterparts, and that capability should be available at their desktop workstations. The Federal law enforcement community should significantly expand electronic connectivity among its intelligence analysts. Each analyst must be provided with the appropriate hardware and services (ranging from simple e-mail connectivity and Internet access to real-time, multimedia collaboration) at the appropriate level of security (ranging from Unclassified to Top Secret).

F-4. Accelerate Federal Law Enforcement Automation Initiatives: The Departments of Justice and Treasury, and Federal law enforcement agencies, will accelerate, to the extent possible, multiyear initiatives upon which they are already embarked that will automate their future reporting and case file systems and convert their active case paper files initiated within the past 10 years. Currently, within the Department of Justice, DEA, FBI, and other components each have their own messaging, case file, and database systems. In Treasury, the U.S. Customs Service, the Internal Revenue Service (IRS)-Criminal Investigations, and other components have their own messaging, case file, and database systems. The databases are mainly indices of individuals with references to supporting case files. The indices also serve as pointers to, and case deconfliction systems for, agents. Case and drug intelligence reporting remain paper intensive, with much of the information located in hardcopy case files at agency field offices.

F-5. Expand Connectivity of NDPIX: All appropriate Federal law enforcement agencies, to include DEA, FBI, U.S. Customs Service, U.S. Marshals, the Bureau of Alcohol, Tobacco, and Firearms, the Immigration and Naturalization Service, and the Border Patrol, plan to participate in the NDPIX system within two years. Expanded connectivity and automation will also be used to accelerate the input of state-level data. The architectural plan will address other requirements for NDPIX, such as a simultaneous input capability for NDPIX and RISSNET.

F-6. Provide Information Technology Support to NDIC: To the degree funds become available:

- (1) Provide secure Internet-type connectivity to other counterdrug centers at the Unclassified level, as well as to CDX for administrative communications, and, in coordination with the Justice Training Center, develop and deliver on-site and video distance learning-based drug analysis education and training;
- (2) Provide Secret connectivity from the analysts' desktops to ADNET via secure firewall;
- (3) Improve access to multiple (and additional) databases via desktop PCs, including direct access to participating agencies' online databases and report transmission systems;
- (4) Provide electronic collaboration capability to NDIC and the Intelligence Community for the purpose of better coordinating annual drug threat assessments and the integration of foreign and domestic strategic drug intelligence analyses;
- (5) Provide the necessary systems connectivity for NDIC to coordinate and manage an online national drug intelligence library and make it available to the counterdrug community; and,
- (6) Provide a method and establish parameters by which to enter Document Exploitation (DOCEX) information into NDIC and agency databases.

F-7. Provide Information Technology Support to EPIC: To the degree funds become available:

- (1) Provide secure Internet-type connectivity to other counterdrug centers, as well as to CDX, at the Unclassified level for administrative communications;
- (2) Provide Secret-level connectivity from EPIC analysts' desktops to ADNET via a secure firewall;
- (3) Upgrade the EPIC Watch by augmenting the current telephonic inquiry system with a system that allows posting of electronic database inquiries via RISSNET, NLETS, and other appropriately secure systems;
- (4) Provide technological connectivity to improve the ease by which state and local law enforcement components can request EPIC services;
- (5) Make the FinCEN-sponsored Suspicious Activity Reports System (SARS) database available for searches by appropriate EPIC personnel;
- (6) Develop a systematic process for state and local law enforcement agencies to collect and report area drug seizure data to EPIC for national tabulation; and,
- (7) Receive Federal U.S. District Court indictment information via the Justice Consolidated Office Network (JCON) or other available means.

F-8. Provide Information Technology Support to FinCEN: To the degree funds become available:

- (1) Provide secure Internet-type connectivity to other counterdrug centers, including CDX, at the Unclassified level for administrative communications;
- (2) Provide secure collaboration capability to FinCEN, other Federal law enforcement agencies, and the Intelligence Community for the purpose of producing interagency illicit financial activities assessments; and,

- (3) Provide FinCEN analysts with improved direct and timely access to Intelligence Community reporting on known or suspected drug-related financial transactions;

F-9. Develop HIDTA Intelligence Centers Systems Standards: ONDCP and the Departments of Justice and Treasury, in coordination with CDX and the Global initiative, will develop minimum systems standards for HIDTA Intelligence Centers, including:

- (1) Wide-area network connectivity between each HIDTA Intelligence Center and the member agencies they serve, including analytic tools, e-mail, Web access, and collaboration capabilities;
- (2) The identification of, and adherence to, compatible systems standards across HIDTAs to ensure information-sharing capability;
- (3) The need for baseline systems in each HIDTA Intelligence Center (for example, ADNET, NDPIX, and event and case deconfliction systems);
- (4) Connectivity between each HIDTA Intelligence Center and its RISS;
- (5) Enhanced electronic connectivity from HIDTA Intelligence Centers to Federal, state, and local law enforcement agencies and national centers;
- (6) Methods for timely pointer information entry into NDPIX; and,
- (7) A photo-imaging network capability that will permit Federal, state, and local jurisdictions to share arrest photographs and biographic data for arrestees in the area. These efforts should comport with the National Crime Information Center 2000 and the Integrated Automated Fingerprint Identification System planned to provide digital photo imaging capability.

F-10. Improve Personnel Development and Training:

- (1) Provide means for the Justice Training Center to collaborate with Treasury's Federal Law Enforcement Center, the HIDTA Assistance Center, the Joint Military Intelligence Training Center, the interagency Training for Intelligence and Law Enforcement Program, NDIC, and other national centers; and,
- (2) Develop a long-distance learning network (with video teleconference training capability) for the JTC.