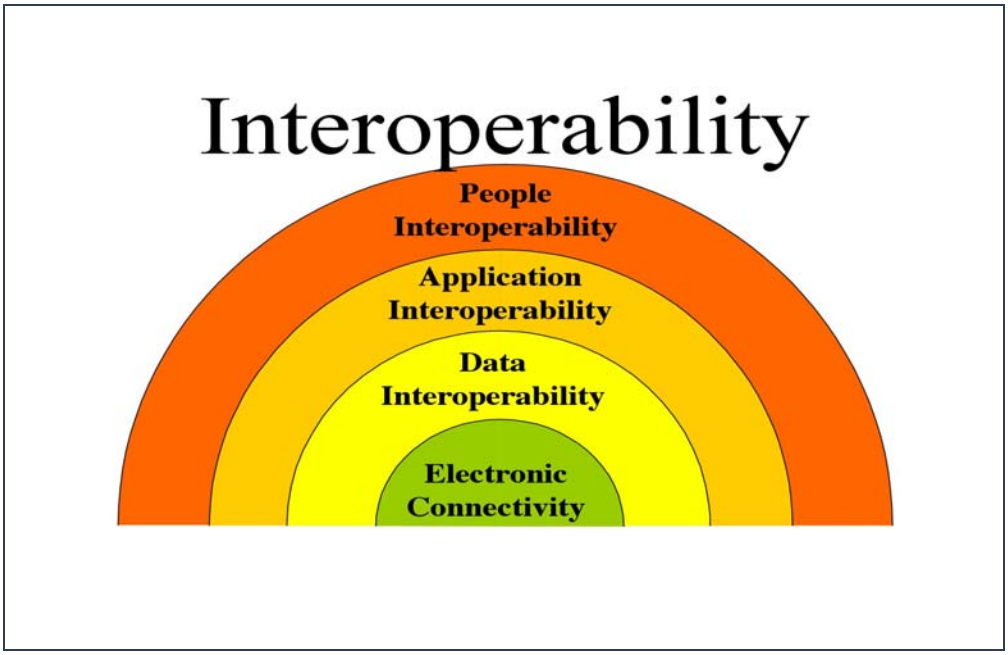
A. Overview

The DMIA of 2000 mandated the Task Force to evaluate and make recommendations on enhancing information technology (IT) systems and data collection/sharing. In June 2002, the DMIA Task Force contracted IT consultants from Los Alamos National Laboratory (LANL) to examine IT systems involved in border management and provide suggestions for a more effective use of technology. They have reviewed 50 key systems from DHS, DOS, and DOJ. A summary of these findings and concepts is included as Appendix F of this report.

In June 2003, LANL hosted a workshop on interoperability and decision support for U.S. border management. Technical representatives from agencies involved in border management, Task Force members, and congressional staff attended. Researchers from the three National Nuclear Security Administration (NNSA) laboratories, Lawrence Livermore, Los Alamos, and Sandia made presentations. The object of the workshop was to bring together Task Force members and individuals who represent the agencies involved in border management with researchers of interoperability and decision support technologies. One of the desired goals was to reach some common ground when referring to these technologies and how they might be used in border management. The workshop was broken into several key sessions focusing on data, application, and people interoperability along with other technologies that might be applicable in this domain. Electronic connectivity was discussed briefly in recognition of the fact that it is the first step of the interoperability process. Each step depends on the prior step to work.



Electronic Connectivity: Electronic connectivity is the communication hardware backbone. The first step in the interoperability process is the ability for two or more systems to exchange information electronically. To do this, the network and communication infrastructure must be in place. Many technologies facilitate this type of communication, but the internet protocol (IP)

dominates. Security layers and access control mechanisms can be laid upon the IP foundation. Most of these solutions lie in dedicated hardware.

High-level statement: Electronic connectivity should to be rapid, consistent, and decentralized.

Data Interoperability: Data interoperability includes data access, format, standards, definitions, quality, etc. Information systems represent data in many different ways, often with different names, structures, and models for the same data. Data interoperability breaks down these independently structured information systems and allows access to their data. Data integration is an automated method for querying across multiple databases in a uniform way. Achieving this integration requires mapping necessary information from each legacy system into a common plan and transforming the information so that when a user queries, the data integration system reformulates it into a query for all the data sources and executes it.

High-level statement: Successful data interoperability depends on standards, quality, and robust search/access technologies.

Application Interoperability: Application interoperability refers to system structures that enable, permit, encourage, monitor, and direct diverse application environments to work together. In application integration, individual applications become components of a larger infrastructure, a framework that can use "middleware"[49] to mediate between the systems and connect the components. Independently designed applications are made to work together to resolve syntactic and semantic differences, organize data, conduct pattern analyses, and find connections in databases of disparate information.

High-level statement: Application interoperability will be enabled through highly functional linkages, careful attention to constraints, and well-designed implementation projects.

People Interoperability: People interoperability refers to the capability of the users, data collectors, and auditors to readily access, interpret, and apply the information provided by relevant sources. Tools alone are not the solution. The people using the tools create the solution. The concepts, software, and hardware are high on the list of importance; however, the role of the human being cannot be replaced. Tools equip human beings to make the critical decisions by filtering, integrating, and/or presenting the data, eliminating the noise, and modeling and simulating systems and scenarios. Making more information available is not an improvement if analysis bottlenecks prevent decision makers from acting on the information in an appropriate and timely manner.

High-level statement: Cooperation and coordination between organizations involved in and affected by U.S. border management activities will enable the nation to take advantage of technological improvements, to address consequential security issues, to maintain international trade health, and to enable the success of end-users, people.

[49] Middleware is software and/or applications used to mediate between systems, providing for interoperability.

B. Findings

Summary Evaluation of IT Systems

The LANL technical team was assigned the tasks of evaluating specific performance and application characteristics of the information systems currently deployed as part of U.S. border management operations. The specific performance areas of interest to the DMIA Task Force include the following:

1. **Purpose:** Clear outline of the purpose(s) for each individual system;
2. **Interface:** How, or if, each system interfaces with other systems in use;
3. **Prospect/Feasibility of Continued Use:** Determine the prospect of continued use of each individual system in context of overall border management systems;
4. **Duplication/Overlapping:** Identify duplicate or overlapping functions or responsibilities among the systems;
5. **Technological Obsolescence:** Determine which systems currently are, or will soon be obsolete. Systems judged to be technologically obsolete should be carefully considered for upgrade, enhancement, or replacement as part of the routine course of responsible system stewardship;
6. **Integration:** Determine (a) which systems are integrated (either fully or partially and (b) which systems could be modified or enhanced and ultimately could become integrated; and
7. **Biometrics:** Determine (a) which systems currently employ biometrics and (b) which systems could employ biometrics.

Discussion of Findings

The evaluation characteristics outlined above touch on important and consequential issues of effective border management operations. The fundamental goals of border management systems are to eliminate the possibilities of activities, persons, equipment, and/or materials breeching U.S. borders with the intent to do grave harm, to facilitate the flow of legitimate enterprise activities, while protecting the privacy of the individual(s). The LANL technical team assessed each system selected for evaluation in light of this goal—knowing the stated purpose of the system and understanding the significance of its purpose relative to the overall border management goals.

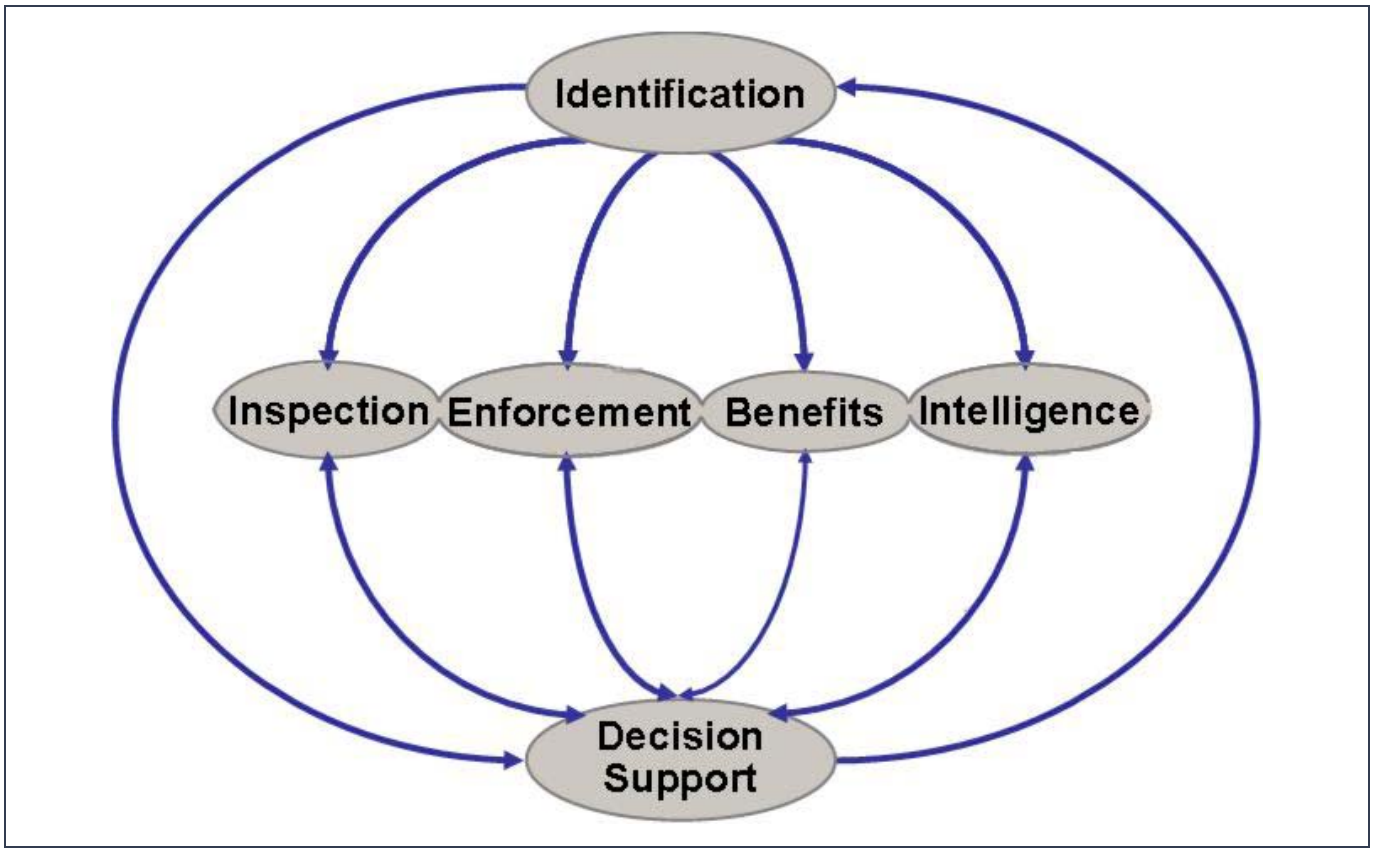
Purpose

As discussed earlier, the 50 individual systems have been identified for evaluation relative to the performance characteristics summarized above. The relatively large number of systems suggests that a purpose-based categorization would help to better organize our detailed assessment. The 50 systems fall naturally into eight specific categories or domains, representing the general purpose they serve. We have placed the systems in the most appropriate domain category, although some of the systems could fall in more than one

functional domain category. The eight categories including the systems assigned thereto are as follows:

- **Identification:** Systems that assist in establishing or determining the identity of persons.
- **Inspections:** Systems that help to verify the identity of persons wishing to enter the county.
- **Enforcement:** Systems that provide case management for violations of U.S. law by foreign nationals.
- **Benefits:** Systems that track and maintain the status of non-immigrants applying for various services or benefits.
- **Intelligence:** For the purposes of this report, systems that analyze information, often drawing and assembling “lookout” records that would result in more detailed inspection.
- **Decision Support:** Systems that provide analysis from enterprise data.
- **Cargo:** Systems that address the importation and movement of cargo.
- **United States Coast Guard (USCG):** Systems that monitor commercial vessels and USCG operations.

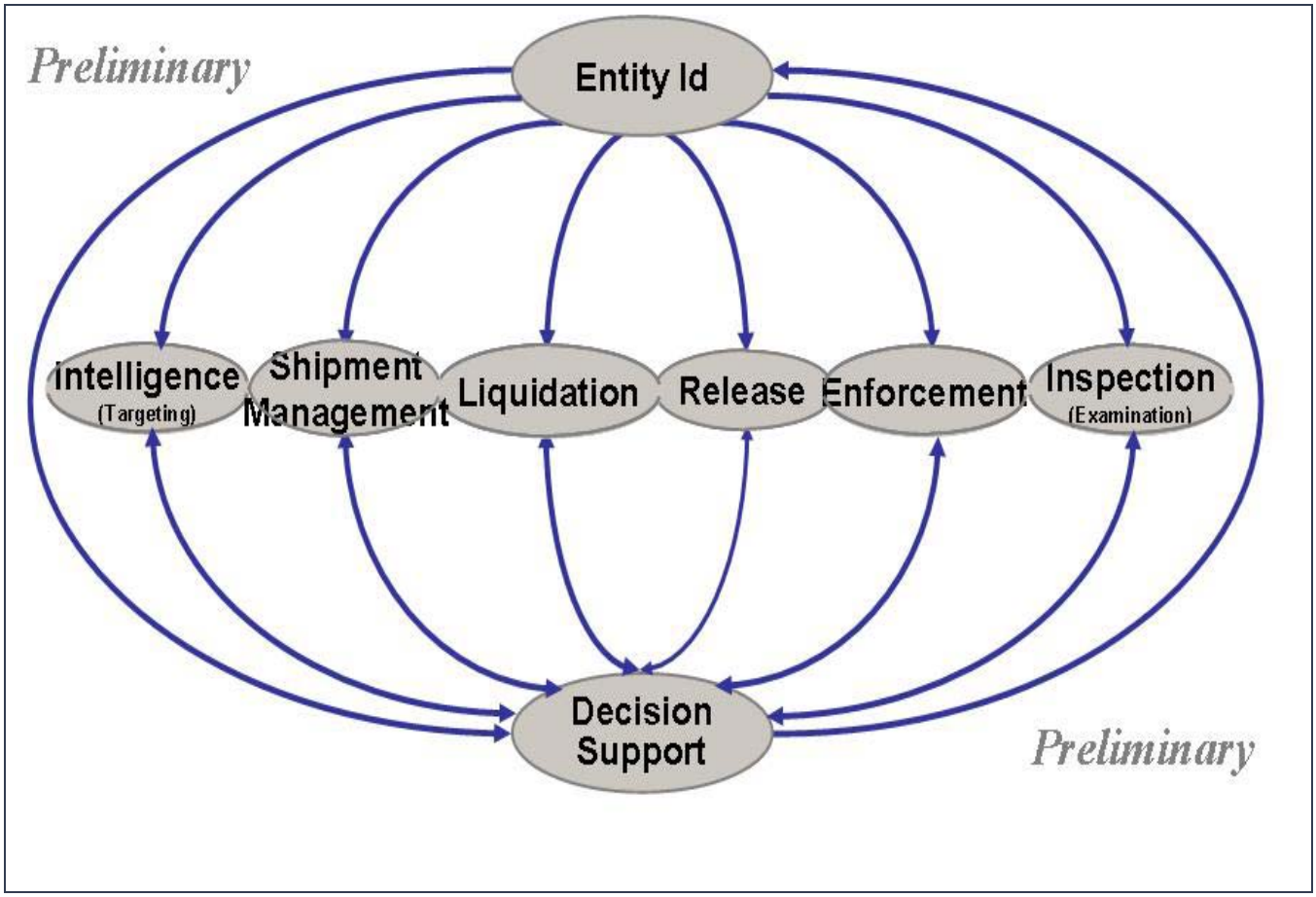
The following diagram illustrates a conceptual interrelationship between the functional domains of the traveler systems.



For the cargo systems, a similar conceptual system is in an early draft stage. It contains many categories similar to the traveler system, and it recognizes the fact that the two systems overlap in several areas. **This work is very preliminary at this time**. The categories for cargo systems are as follows:

- **Entity ID:** Systems that support and maintain the creation of electronic identification of organizations and other entities associated with cargo importation.
- **Inspection/Examination:** Systems that support the inspection and/or examination process of cargo.
- **Enforcement:** Systems that deal with case management when laws have been violated while importing cargo through the border.
- **Release:** Systems that handle the information associated with the release of cargo once it has been inspected and/or examined.
- **Liquidation:** Systems that deal with the transactions for the liquidation or payment of import duties.

- **Shipment Management:** Systems that allow the preparation of all required documentation to import cargo.
- **Intelligence (Targeting Systems):** For the purposes of this report, systems that analyze patterns and trends to identify cargo requiring more detailed inspection.
- **Decision Support:** Systems that provide analysis from enterprise data.



LANL will continue to explore these cargo systems with the appropriate entities to further a conceptual interface for these cargo systems and, where appropriate, overlaps with the conceptual traveler systems.

Interface

The systems evaluated show a wide range of interrelationships. For example, a criminal history information system shares information with a number of agencies, including the FBI, various criminal justice agencies, and appropriate courts. Information from inspection operations is subsequently transferred to an enforcement system, a decision support system, a benefits system, another intelligence system, and an identification system.

Prospect/Feasibility of Continued Use

The LANL technical team used the design and software implementation of each system to evaluate feasibility of continued use. Exceptional design enables systems to accommodate changes and enhancements and incorporates industry standard technologies. Four systems are noted for their **exceptional** design, software implementation, and overall usability. Two specific systems could be reasonable candidates for continued use if they were to receive software upgrades. Updating this software to a more modern operating system would be reasonably straightforward.

Some of the system managers the LANL technical team interviewed spoke of plans to upgrade and enhance system performance capabilities. It is assumed that timely improvements will be made to these systems as scheduled.

Duplication/Overlapping

Duplication and/or overlapping characteristics imply that certain systems serve the same purpose, replicate certain functionalities, or have been replaced with other capable systems. It is not surprising that a number of these systems are considered obsolete. It is reasonable to expect that the functionality of obsolete systems has migrated to other, more modern systems and, therefore, overlap with them.

Some identification systems and some lookout databases appear to have a natural clustering of overlaps. It is likely that their functionality is better served by integrating them. Two systems have a closely shared relationship, suggesting consolidation of these two systems should be investigated.

Technological Obsolescence

Obsolescence is a state or condition relative to the “modernity” of the technology compared to current, best practices. It is misleading to assume that because certain systems are deemed technologically obsolete that they should be quickly removed from service, that they are less than adequate, or that they are “pitifully weak” systems. Systems can be fully satisfactory in terms of the information they provide while at the same time technologically obsolete. The nature of obsoleteness means that systems judged to be technologically obsolete should be carefully considered for upgrade, enhancement, or replacement as part of the routine course of responsible system stewardship.

We evaluated the information systems relative to their technical and/or design obsoleteness. Systems were considered **technologically obsolete** if the hardware supporting the system is no longer routinely maintained by private industry, and/or the operating system has been generally replaced by more comprehensive capabilities. The **design** of a system is considered obsolete if the model of the procedures and data does not accommodate changes and enhancements. For example, if the design of a system does not permit the straightforward and/or cost-effective changes/additions of normal business rules, then the system is deemed obsolete.

The majority of systems the LANL technical team determined to be obsolete have technological deficiencies. However, two systems are uniquely obsolete in both design and technology. Because modern capabilities have replaced a number of these systems, it may be prudent to develop a plan for removing/replacing these systems in an orderly fashion. The systems considered "partially" obsolete merit immediate upgrading.

Integration

Integration means that the systems function together in a unified manner to accomplish the objectives of border management activities. The system integration characteristics of each of the systems were determined based on generally good business practices, overall security requirements, and unified system performance expectations. A total of 20 systems are judged as **adequately[50] integrated;** nine systems are judged as **partially[51] integrated**; and nine are judged as **minimally[52] integrated**.

- Of the currently **adequately integrated** systems, three have the potential for limited integration in the future. All of the other systems that are currently adequately integrated can be incrementally integrated as required for the foreseeable future.

- Only two of the systems currently **partially integrated** offer the potential for a more comprehensive level of integration.

- Five of the **minimally integrated** systems can be integrated well beyond what they are now.

- Two of the systems that are not currently integrated may be more fully integrated.

Biometrics

Biometrics is the automated methods of identifying or authenticating the identity of living persons based on physiological or behavioral characteristics. Biometrics includes facial photographs, fingerprints, hand geometry, voice recognition, and many other unique human identifiers. Fourteen existing systems incorporate at least some degree of biometrics as part of the system configuration.

The biometric information most of the systems use includes photographs or fingerprints. All of these systems have significant potential for greatly expanded use of biometric identifiers. Although the advantages of multiple biometric information sets have not been rigorously quantified, it appears that biometric diversity may enhance the quality of person identification and/or validation systems. (Refer to Consideration 3 later in this chapter.)

[50] Adequately integrated systems are blended together in a manner consistent with the operational expectations of the sponsoring organization.
[51] Partially integrated systems have a limited degree of integration within the operational domain that they were designed to serve. They could be more effectively integrated today.
[52] Minimally integrated systems have not been systematically integrated.

Observations

Observation 1: Transfer/exchange diversity limits information quality.

The wide range of data transfer connections could seriously hamper the timeliness and availability of critical information to the relevant systems. The potential propagation of errors, the variations of definitions among the systems, the limitations imposed by law, the differing system priorities, and the lack of centralized oversight help create this limitation.

Observation 2: As anticipated, essentially all of the systems examined manage/manipulate information.

With few exceptions, the systems of interest do indeed acquire, maintain, and post large amounts of information. It is worth noting that the fundamental technology by which information management is accomplished differs little between the various systems. Most are built upon linear data construction techniques together with “key word” searchable file structures.

Observation 3: Obsolete systems are notably populated by overlaps and duplications.

The majority of systems determined to be obsolete also have overlapping or duplicative operational capabilities. This implies that system overlaps are at least partially attributable to unmitigated obsolescence. Experience has shown that system-wide inefficiencies are more likely to occur if effective modernization strategies are not routinely implemented.

Observation 4: Most systems are obsolete because of platform problems.

Almost without exception, obsolete systems are implemented using outdated technologies, i.e., mainframe computational systems. The likely consequences of technological obsolescence may include significant maintenance costs, extremely limited interoperability, and little, if any, adaptability.

Observation 5: Most systems are or readily could be integrated.

Over 80 percent of the systems evaluated were found to be at least “minimally” integrated and, almost without exception, system-by-system implementation technologies do not prevent integration enhancements. This is very good news; however, it is noted that domain-wide “functional integration” needs to be evaluated because it is much more consequential than individual “system-by-system integration.”

Observation 6: Biometric identifiers have been implemented across a broad range of appropriate applications. Most systems are designed to accept biometrics in a reasonably straightforward manner.

There are no glaring deficiencies relative to the use of biometric identifiers. There is the obvious opportunity to enhance the use of biometrics within most of the systems to improve the quality of person identification results.

Observation 7: The efficacy of the information ultimately posted by each individual system is inseparably coupled to the quality of the data resident in the system's data sources.

The successful application of the information management capabilities summarized in this report ultimately depend on the accuracy, completeness, timeliness, and relevancy of the source data upon which these capabilities are built.

Observation 8: Four systems have exceptional design, software implementation, and overall usability.

These systems clearly represent exceptional information technology implementation. These systems should form the core element from which evolving information systems are derived to meet the demands of the future.

Observation 9: Modern communication technologies have not been fully exploited by any of the border management systems.

Modern information technologies have developed remarkably diverse and useful techniques for communicating complex information to people. These technologies include digitized voice transmissions, animations, graphics, tabulations, iconic representations, multidimensional virtual environments, three-dimensional engineering plots, geographically correct simulations, site-specific GPS-connected locators, etc. Many of these technologies offer communication environments that are selectable by the end-user. Consequently, the end-user can select the communication environment(s) that works best for his/her situation. In fact, the selection process can be keyboard activated (the traditional approach), voice activated (keyed to individual voice patterns), or activated by specific person biometrics such as eye-retina movement.

Observation 10: Robust information technologies depend on robust infrastructures for successful implementation.

Even the best of information technologies cannot be realized if the infrastructure upon which it is deployed is less than adequate. **The current support infrastructure is not sufficiently robust to sustain broad information technology deployment.** (Specific, localized elements, however, are somewhat adequate.) Infrastructure elements include high-speed, high-capacity transmission systems (including satellites), workstations, data storage and access systems, ergonomically compliant communication hardware, information input/output systems, and security-compliant encryption systems.

Observation 11: Technological obsolescence is not a small problem. A third of the systems have notable technology and/or design modernization challenges.

Information systems that become obsolete are not necessarily useless or unsatisfactory. Operational systems that are technologically obsolete reflect as much on the attitude and style of the organizational support managers as it does on the system itself. Getting along with "old" technology is risky. Old systems tend to be well suited for operational conditions that no

longer exist. Old systems are not likely to be prepared for surprise situations, emergencies or rapidly changing national priorities. One-of-a-kind technologies are very costly (in more than just dollars) to repair, maintain, and, ultimately, to replace.

Considerations

Consideration 1: Personal privacy information must be rigorously protected.

It is essential to the successful implementation of modern IT systems that the privacy of personal information and all associated data be scrupulously protected from unauthorized access, use, disclosure, or manipulation. Access control technologies should be used to (1) verify authorized users; (2) detect and track unauthorized access; (3) monitor information manipulation activities; (4) encrypt information transfers; and (5) encrypt information electronically stored.

Administrative controls include authorization documentation, routine investigations/audits, ID badges, background checks, password controls, two-person rules, and physical access controls.

Suggested Actions:

- Determine and verify applicable personal privacy laws, policies, procedures and requirements;
- Develop and validate personal privacy implementation plans;
- Extensively field-test privacy controls;
- Implement privacy control system; and
- Routinely maintain, evaluate, test, modify, and upgrade system.

Consideration 2: Consistent with privacy considerations, address the security advantages of understanding the consequences of persons' and organizations' long-term behavior.

If the full benefits of modern information technologies are to be realized, it is absolutely essential to track and assess activity patterns of individuals over relatively long periods of time (more than 25 years), recognize and understand person-by-person behavior patterns, and track person-to-person linkages, contacts, and often subtle interrelationships. Highly integrated, domain-wide systems should be designed and built to assess the implications of long-term behavior patterns.

Suggested Actions:

- Establish agreements between relevant agencies;
- Develop, accept, verify, validate, and implement information standards;
- Develop and/or modify applications;
- Deploy system-wide;
- Evaluate, maintain, and upgrade routinely; and
- Maintain consistency with privacy considerations.

Consideration 3: Determine the security implications of interagency integration schemes.

The integration condition of the systems reported herein was determined based solely on each individual system. Extensive analysis should be performed of the security implications associated with broad, system-to-system integration. It is believed that domain-wide integration across many agencies and organizations has the greatest security value to border management operations. The extent to which domain-wide integration may play an important role in security enhancement must be robustly defined before chartering major programs with the intent to upgrade the performance of the nation's technology-enabled security systems.

Suggested Action: Evaluate simultaneously with actions suggested under Consideration 2, above.

Consideration 4: Rigorously assess the value of multiple biometric measures.

It is not clear that multiple biometric benchmarks actually improve person identification, detection, and/or validation. Factors affecting this include varying levels of technological maturity and the intended use of the biometric. Rigorous analyses should precede a national commitment to large scale, domain-wide biometric deployments to do the following:

- Carefully assess which biometric technologies actually add value [combined as well as individualized biometric technologies];
- Determine the breadth of domain-wide deployment that makes sense;
- Recommend implementation strategies based on population characteristics;
- Estimate implementation costs (capital, operating, and maintenance) as a function of implementation strategy; and
- Recommend a long-term plan for taking advantage of biometric technologies when they become available.

Suggested Actions:

- Perform analyses of biometric applicability as outlined above;
- Validate LANL technical team assertion that biometrics offer the most return on investment for two situations, i.e., self-identification at enrolled POEs and identification of high-risk person;
- Evaluate and validate biometric advantages within other border management environments; and
- Support maintenance upgrade activities particularly as the science of biometrics matures.

Consideration 5: Proactively avoid systematic technological obsolescence.

Dealing with technological obsolescence is an ongoing challenge facing industry, academia, and government agencies. Planning that includes the routine assessment, justification, and the ultimate **timely** upgrade (or removal) of key information systems should be an integral part of all operational activities, funding strategies, and organizational responsibilities associated with homeland security assignments. **Technological obsolescence should not be permitted for systems essential to the security of the nation.**

Suggested Actions:

- Identify well-maintained systems;
- Determine proven maintenance strategies;
- Coalesce exceptional maintenance strategies into prioritization principles;
- Maintain, upgrade, or replace systems per principle-based guideline; and
- Routinely assess/improve robustness of maintenance implementation strategies.

Consideration 6: Ensure the quality of the data that supports database systems.

The value of information is inseparably coupled to the legitimacy of the data upon which the information is extracted. The quality of the data sources supporting the information technologies must be managed in partnership with border management system improvements. Data verification and validation technologies should be rigorously assessed, developed, and deployed in concert with modern information management strategic upgrades.

Suggested Actions:

- Identify, categorize, and evaluate data sources;
- Identify and/or specify technological assets for data source verification and validation;
- Develop data quality management strategic plan;
- Execute data quality plan, document lessons learned; and
- Routinely assess/improve data management quality processes, technologies, and implementation of strategic plans.

Consideration 7: Streamline access to information.

Access to relevant information in a timely fashion is an essential element of border protection operations. Systems designed to provide the necessary information should avoid complex interconnections and the current excessively diverse data sources. Standardization of information protocols including centralization of data quality maintenance and the dissemination infrastructure should be part of the organizational improvements established by DHS. Modern communication technologies should be extensively deployed to enhance information clarity to all frontline decision makers such as USBP agents and CBP officers.

Suggested Actions:

- Identify and prioritize data access and interconnection requirements;
- Determine optimum standardization approaches;
- Coordinate with data quality management systems per Consideration 6, above;
- Develop strategic implementation plan for communication technology deployment;
- Implement plan to maintain, upgrade, and replace systems and support infrastructure as required; and
- Routinely assess strategy based on feedback from "the field," on research and development progress, and on national priorities.

Consideration 8: Ensure "new" systems are designed to easily accommodate change.

The development of a national strategy for applying modern information technologies to border management issues is an essential part of achieving national security objectives. It is anticipated that "new" data systems, applications, and other tools will be deployed as a result of an integrated approach to border management activities in the future. Every effort should be made to assure that "new" systems are designed with change in mind. For example, the business rules and/or processes that determine how entry is to be accomplished should not be hard-coded into new or upgraded information technology tools.

Suggested Actions:

- Form integrated systems development strategy matching the national strategy for modernizing information technology applications;
- Set design standards for information tool design and deployment consistent with adaptive data management concepts;
- Provide development guidelines based on software quality assurance principles; and
- Provide incentives for meeting adaptive design standards and quality assurance principles.

C. Task Force Observations of Information Technology

In the course of various site visits, the Task Force made the following observations in the area of IT interoperability.

- Concerns include privacy issues and balancing enforcement and commerce.
- Public concern with government handling of personal and proprietary data has resulted in legislation and judicial decisions to prohibit the release and use of many kinds of sensitive information about individuals and businesses. Information systems must include safeguards against inappropriate use and release of such information to be consistent with the law.
- Technology advances needed at seaports to address projected increase in cargo container volume. Leverage technology to help law enforcement differentiate between legitimate and suspicious cargo.
- Agencies need to share information in a responsible way, with appropriate levels of access. Currently, exchange of information is limited and not all information can be shared electronically.
- New/improved systems' interaction with private sector partners, who may have differing technology levels, need to be reviewed. Systems should use consistent interfacing using appropriate technologies that still achieve required security and data-sharing needs.
- At security and trade admissibility decision points, real-time, all-inclusive data availability is paramount with no exceptions.
- The ultimate goal in terms of documentation is a secure, machine-readable, multi-faceted document capable of storing multiple biometrics for an individual.
- Entry-exit/US-VISIT is a critical component of a broader DHS strategy, and any system that is designed or perceived as a stand-alone system simply will not fit into a post-September 11, 2001, world.
- Training, enrollment, and maintenance costs must also be considered and funded as part of any costs associated with use of biometrics.
- All major technology enhancements/additions must be field tested in rigorous conditions before major operational rollout at POEs where significant negative impacts could be felt.
- Private sector users should be involved, to the extent possible/practicable, in the design and development phases of any IT investments that will require interface with them, so

that compatibility issues can be resolved early, and significant immediate capital investments by the private sector can be avoided.

- Encourage use of synthetic environments, using off-the-shelf technology, in the federal border management system. Synthetic environments will assist in the identification of best practices and weaknesses of border management systems, policies, and procedures prior to implementation and integration into border management. It could benefit not only inspections process and border management, but also as simulation for POE emergency events, security threat scenarios, and first responders. Synthetic environments can be developed with the use of facility blue prints, digital images, and laser measurement.

- Promote the standard use of middleware, as it enhances and maintains interoperability between systems. Prototype studies should be undertaken to asses the issues faced with the use of middleware in the border management domain.

- Encourage border management agencies to research and utilize historical data and analysis to determine likely patterns and/or mitigate threat or threat assessment. Data mining is central to this effort. Data mining is the set of technologies that allows the extraction of information patterns embedded in records or other facts on a data set. These technologies not only allow the identification and extraction of these patterns, but also allow the data to be presented in a usable fashion by decision-makers in the domain.

- Consider the use of image-understanding technology to assist with border management and possibly preclude the need for significant staffing increases between POEs. The technology utilizes remotely mounted or unmanned cameras to analyze captured images, look for objects or events of interest, and perform object recognition, tracking, region-of-interest recording, and economical storage and transmission of selective object information. While this technology is still in its infancy, it has several applications deemed suitable for border management and inspections activities.

- Visual Ergonomics have to be taken into account and their impact on the design of “user centric” interfaces needs to be well understood for implementation on future systems. “Visual ergonomics” can be defined in two different ways: first, is the physical environment between the display and the worker; second, is the design and comprehensibility of information provided to a user. The defense establishment has done a lot of work in this area, particularly as it relates to cockpit activity for next-generation jet fighters. Visual ergonomics is one of the many aspects of people interoperability of how people and systems interface. Human factor studies provide valuable data for implementing good user-centered design and visual ergonomics.

D. Conclusions

The Task Force considered all these issues and has the following specific recommendations:

Recommendation 9

Information technology systems should be enhanced or designed to ensure compatibility and meet the needs of the end-user. This is to achieve effective communication with federal, state, local, and private industry partners.

Recommendation 10

The Federal Government should create an information technology master plan that employs consistent interfacing and appropriate technologies that still achieves required security and data-sharing needs. Such master plan should:

- **Rigorously assess the value of multiple biometric measures;**
- **Proactively avoid systematic obsolescence;**
- **Ensure the quality of the data that supports database systems;**
- **Ensure "new" systems are designed to easily accommodate change;**
- **Leverage technologies currently available to enhance security and facilitation in the border management systems;**
- **Use a pilot project to rigorously field test systems under operational conditions before major rollout at POEs where significant negative impacts could be felt;**
- **Fund critical IT border management modernization systems;**
- **Fund and equip all border enforcement programs with compatible technologies and equipment; and**
- **Protect respondents from public release of proprietary or confidential information.**