IHS National Project Status Sheet

Title	Project Description	Process Approach	Status
GPRA	Under the *Government Performance and Results Act* (GPRA), agencies were required to submit strategic plans no later than September 30, 1997, to the Office of Management and Budget (OMB) and Congress. Updates are required at least every 3 years thereafter. Annually, beginning with fiscal year 1999, agencies must submit to OMB performance plans covering each program activity in the agency's budget. OMB, using these plans, must prepare a federal performance plan for inclusion in the president's annual budget submission to Congress. Reports beginning in fiscal year 2002 must include actual program performance results for the 3 preceding fiscal years.	(1) Annually, IHS must submit to OMB performance plans covering each program activity in the agency's budget. (2) Annually, agencies must submit program performance reports covering performance for the previous fiscal year to the president and Congress. Reports beginning in fiscal year 2002 must include actual program performance results for the 3 preceding fiscal years.	IHS currently submits, as required, an annual Performance Plan, a Strategic Plan, and has developed performance measures to support goals and objectives set forth in all required reporting documents.
PRA	The purpose of the *Paperwork Reduction Act* (PRA) is to minimize the public's paperwork burdens resulting from the collection of information by or for the federal government, to coordinate federal information resource management policies, to improve the dissemination of public information, and to ensure the integrity of the federal statistical system.	PRA requires agencies to indicate in strategic information management plans how they are applying information resources to improve the productivity, efficiency, and effectiveness of government programs, including improvements in the delivery of services to the public. It also requires that all agencies develop and maintain a strategic IRM plan that describes how IRM activities help accomplish agencies' missions.	
GPEA	*Government Paperwork Elimination Act* (GPEA) – Extends the PRA to create more accessible and efficient government, which requires public confidence in the security of the government's electronic information communication and information technology systems. Electronic commerce, electronic mail, and electronic benefits transfer can involve the exchange of sensitive information within government, between government and private industry or individuals, and among governments. Electronic systems must be able to protect the confidentially of citizens' information, authenticate the identity of the transacting parties to the degree required by the transaction, guarantee that the information is not altered in an unauthorized way, and provide access when needed.	Each agency must build on their existing efforts to implement electronic government by developing a plan and schedule that implement, by the end of Fiscal Year 2003, optional electronic maintenance, submission, or transactions of information, when practicable as a substitute for paper, including through the use of electronic signatures when practicable. Agencies must submit a copy of the plan to OMB by October 2000 and coordinate the plan and schedule with their strategic IT planning activities that support program responsibilities consistent with the budget process (as required by OMB Circular A-11).	(1) GPEA plan was submitted to DHHS for inclusion in their GPEA project plan. (2) PKI pilot project is being initiated to develop the policies and practices necessary to implement a public key technology infrastructure.
CCA	The *Clinger-Cohen Act* (CCA) is intended to improve the productivity, efficiency, and effectiveness of fed-	(1) Requires Executive agencies to base decisions about IT investments on quantitative	(1) DIR is the IHS CIO office; (2) the CIO's roles and responsibilities have

IHS National Project Status Sheet

Title	Project Description	Process Approach	Status
	eral programs through the improved acquisition, use, and disposal of IT resources. Among other provisions, it (1) encourages federal agencies to evaluate and adopt best management and acquisition practices used by both private and public sector organizations, (2) requires agencies to base decisions about IT investments on quantitative and qualitative factors associated with the costs, benefits, and risks of those investments and to use performance data to demonstrate how well the IT expenditures support improvements to agency programs, through measurements such as reduced costs, improved employee productivity, and higher customer satisfaction, and (3) requires executive agencies to appoint CIOs to carry out the IT management provisions of the act and the broader information resources management requirements of the Paperwork Reduction Act. The Clinger-Cohen Act also streamlines the IT acquisition process by eliminating the General Services Administration's central acquisition authority, placing procurement responsibility directly with federal agencies, and encouraging the adoption of smaller, modular IT acquisition projects.	and qualitative factors associated with the costs, benefits, and risks of those investments and to use performance data to demonstrated how well the IT expenditures support improvements to agency programs, through measurements such as reduced costs, improved employee productivity, and higher customer satisfaction; (2) requires executive agencies to appoint executive-level Chief Information Officers (CIO); (3) Executive agencies must ensure that information security policies, procedures, and practices are adequate to protect the agency's resources; and (4) Executive agencies must assess, as part of the Results Act strategic planning and performance evaluations.	been established; (3) Performance measures—included in ITIRB process—link IT investments to agency mission and performance (e.g., GPRA); (4) IHS has established an ITIRB to assess and select IT Projects. (5) The DIR continues to provide training on the investment review process and functions of the Information Technology Investment Review Board (ITIRB). The ISAC and ISCs received ITIRB training in August. (6) IT Architecture (ITA) workgroup met in July to further revise and finalize the IHS ITA Plan. (7) Began Chief Information Officer certification through Carnegie Mellon University to develop competency base as contained in the CCA.
Raine's Rules	Under the *Raine's Rules*, which have been incorporated into the CCA, major information systems investments should: (1) Support core or priority federal government missions; (2) be impossible for another agency, company or government to efficiently perform; (3) support work already redesigned to cut costs, improve efficiency and use off-the-shelf technology; (4) show a return on investment equal to or better than other uses of available resources; (5) be consistent with agency and government wide architectures that integrate work and information flows with strategic plans, are year 2000 compliant, incorporate standards allowing information exchange and resource sharing; and retain flexibility in the choice of suppliers;	All eight rules are to guide agencies in proposing IT spending and will be the measures OMB will use to accept or reject proposals.	The ITIRB process adheres to Raine's Rules.

IHS National Project Status Sheet

Title	Project Description	Process Approach	Status
	(6) reduce risk by avoiding custom design, using pilot projects and prototypes, establishing clear measures of success, securing buy-in from users; (7) be put into effect in phased, successive chunks that are short-term and narrow in scope and independently solve part of an overall mission problem; and (8) allocate risk between government and contractor, tie payments to accomplishments and use commercial technology.		
CFO Act	The *Chief Financial Officers* (CFO) Act improves and strengthens financial management and accountability in the federal government. It laid the legislative foundation for the federal government to provide taxpayers, the nation's leaders, and agency program managers with reliable financial information through audited financial statement. It provides a framework for improving federal government financial systems, with a focus on program results.	The CFO Act requires 24 federal agencies to have Chief Financial Officers and Deputy Chief Financial Officers and lays out their authorities and functions. Agencies are required to prepare agency wide financial statements and subject them to audit by the agencies' Inspectors General (IG).	
A-11/A-130 OMB Circulars	*Circular No. A-11* covers the development of the Presidents budget and tells you how to prepare and submit materials required for OMB and Presidential Review of agency requests and for formulation of the FY 2001 Budget. The circular also describes the requirements of the Government Performance and Results Act and tells you how to prepare and submit strategic plans, annual performance plans, and annual program performance reports. Additionally, it discusses the planning, budgeting and acquisition of capital assets, and tells you how to prepare and submit information on new and past acquisitions. *Circular No. A-130* provides uniform government-wide information resources management policies as required by the Paperwork Reduction Act of 1980.	Circular No. A-11 requires: (1) agencies must explain the program requirements that necessitate advance appropriations; (2) agencies need to identify specific human resources management and development objectives and associated resources; (3) agencies need to reflect both the Federal Physicians Comparability Allowance Amendments of 1987 and the Federal Employees Healthcare Protections Act of 1998 when determining physicians comparability allowance; (4) agencies need to ensure that electronic and information technology acquisitions meet the requirements of the Rehabilitation Act of 1973 with respect to accessibility for individuals with disabilities; (5) agencies need to submit some materials by September 11th or other date specified by OMB; (6) agencies need to discuss grants management in the budget justification materials Circular No. A-130 requires:	

IHS National Project Status Sheet

Title	Project Description	Process Approach	Status
		(1) Agencies shall plan in an integrated manner for managing information throughout its life cycle; (2) Provide for public access to records where required or appropriate; (3) Agencies shall collect or create only that information necessary for the proper performance of agency functions and which as practical utility; (4) Agencies shall use electronic collection techniques where such techniques reduce burden on the public, increase efficiency of government programs, reduce costs to the government and the public, and/or provide better service to the public; (5) records management; (6) provide information to the public consistent with their missions; (7) Agencies shall maintain and implement a management system for all information dissemination products; (8) avoid improper restrictive practices; and (9) Agencies shall use electronic media and formats, including public networks, as appropriate and within budgetary constraints, in order to make government information more easily accessible and useful to the public	
PDD-63	The *Presidential Decision Directive 63* (PDD-63) on Critical Infrastructure Protection (CIP) calls for a national effort to assure the security of the increasingly vulnerable and interconnected infrastructures of the United States. Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private.	Every department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems. Every department and agency Chief Information Officer (CIO) shall be responsible for information assurance. Every department and agency shall appoint a Chief Infrastructure Assurance Officer (CIAO) who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure. The CIO may be double-hatted as the CIAO at the discretion of the individual department. These officials shall establish procedures for obtaining expedient and valid authorizations to allow vulnerability	(1) The IHS CIO has been designated as the CIAO; (2) Vulnerability assessments of IHS's critical computer systems and network will be a part of the upcoming Certification and Accreditation (C&A) process.

IHS National Project Status Sheet

Title	Project Description	Process Approach	Status
		assessments to be performed on government computer and physical systems. IHS did not meet the national criteria for Critical Infrastructure Protection. However, IHS infrastructure is critical to the IHS's mission for the delivery of health care. Therefore, IHS will proceed with its own, internal, CIP project.	
Section 508	*Section 508* requires that Federal agencies' electronic and information technology is accessible to people with disabilities, including employees and members of the public.	All Federal agencies and departments must report to the Attorney General by June 15, 1999, the extent to which their electronic and information technology is accessible to and usable by people with disabilities.	(1) IHS-hosted Web pages have been reviewed for compliance with Section 508. (2) Section 508 report was submitted
HIPAA	The Health Insurance Portability and Accountability Act (HIPAA) is divided into the following parts: (1) insurance portability; and (2) Administrative Simplification, which in turn consists of: (a) Standardization of health information transactions and coding (b) Privacy (patients rights regarding access, use, and disclosure of personal health information, and the patient's right to sue) (c) Security (assurance of the confidentiality, integrity, and availability of information)	(1) Requires the appointment of an agency Privacy Officer (2) Requires the appointment of an agency Security Officer (3) HHS has issued a Privacy Rule (effective date on hold) (4) HHS has issued a proposed Security Rule (effective two years after the final rule is issued) "Each entity…must assess potential risks and vulnerabilities to the individual health data in its possession and develop, implement, and maintain appropriate security measures…"	(1) IHS is continuing its implementation and use of transaction and coding standards (2) IHS is in the process of performing a security assessment in connection with its C&A process (3) Security requirements for HIPAA, OMB A-130, HCFA, and other mandates analyzed so that a coordinated approach can be taken. (4) Policy requirements identified to establish policy foundation to support compliance with HIPAA. (5) Senior Staff briefing presented to provide specific recommendations for initiating a coordinated national approach for HIPAA compliance. (6) HIPAA program track will be included in Information Technology and Business Conference to be conducted in mid-July. (7) The CIO prepared background materials to get the IHS ready internally to address HIPAA issues including an Action Memorandum designating Dr. Robert Harry as the HIPAA lead for IHS in February. (8) The CIO and Dr. Harry attended a JCAHO-sponsored meeting on how the accreditation process will support HIPAA compliance in February. (9) DIR gave a Public Key Infrastructure (PKI) briefing to an interagency health care work-

IHS National Project Status Sheet

Title	Project Description	Process Approach	Status
			ing group. There is potential for funding of a shared PKI project between the VA and IHS. The PKI effort will affect RPMS, NPIRS, GPEA, and HIPAA requirements
PKI	Public Key Infrastructure (PKI) is a technology that provides the following benefits: (1) **Strong authentication —** The use of digital certificates signed by a trusted authority provides convincing assurance of the user's identity. (2) **Message confidentiality and integrity —** Once encrypted, messages which are altered will not decrypt properly. Therefore, any message which properly decrypts is guaranteed to be unchanged. (3) **Non-repudiation —** Only a message encrypted with an entity's private key will decrypt with that entity's public key, and visa versa. Therefore, if a message is properly decrypted using an entity's public key, the message had to have been encrypted by that entity's private key. A trusted Certificate Authority (CA) issues a signed digital certificate to an entity following verification of that entity's identification. The digital certificate contains the entity's public key. At the same time, a private key—which will be securely stored—is issued to the entity. The public and private keys are mathematically related such that: (1) A message encrypted with either key will be successfully decrypted by the other. (2) Neither key can be determined from the other. PKI implementation will provide the necessary technology infrastructure required by the security and privacy provisions of HIPAA and GPEA.	The IHS PKI Pilot Project is a joint DoD, VA, and IHS pilot project under the auspices of the Government Computer-Based Patient Record (GCPR) project. (1) In the first phase, the participants will establish appropriate policies, define necessary practices, and install and test enabling technologies for a Public Key Infrastructure. These PKI policies, practices, and technologies must be compatible with the GSA Federal Bridge Certificate Authority (FBCA). (2) In phase two, security tokens (smart cards, keys, fingerprint readers, etc.) to enable two-factor authentication (two of the three following categories: something you know (passwords, PINs), something you have (token, smart card), something you are (biometric). This two-factor authentication is especially important for Internet access or remote access using dial-up modems. (3) In phase three, one or more existing application packages will be selected for modification to enable programmatic implementation of PKI technologies. Here, techniques for the automated use of PKI to secure file transfers will be explored. This will enable us to develop reliable estimates of the time and resources needed to implement secure transfer of medical information as required by HIPAA, and personal privacy information as required by GPEA.	(1) The project has been planned and organized with the support of Mitretek Corp. (2) The project approach and schedule have been reviewed by Mitretek and selected interested parties within IHS. (3) The project overview was presented to the Health Care PKI Working Group at its February 2001 meeting.
GISRA	The *Government Information Security Reform Act* (GISRA) of 10/30/00 requires that each Federal agency ensure the periodic testing and evaluation of its information security controls and techniques.	(1) develop and implement an agency-wide information security program (ISP) for the operations and assets of the agency, including risk assessments of cyber threats, management testing of cyber security policies and intrusion	Provided status and supporting documentation to DHHS for submission to the House Committee on Energy and Commerce.

IHS National Project Status Sheet

Title	Project Description	Process Approach	Status
		detection and response procedures. (2) annually solicit an independent evaluation of the ISP and practices of the agency (first one by 10/30/01). (3) identify resources needed (budget, staffing, and training). (4) develop procedures for detecting, responding, and reporting security incidents to law enforcement authorities and GSA (FEDCERT). (5) expand insurance of confidentiality, integrity, and availability of Agency's AIS to include features of authentication and non-repudiation. (6) promote security awareness training.	
GCPR	The Department of Defense (DoD), the VA, and DHHS (IHS), have embarked on the *Government Computer-based Patient Record* (GCPR) framework project, a joint effort to improve information sharing and collaborative decision making across the continuum of Federal healthcare. The GCPR framework project's goal is to improve public and individual healthcare by using *existing* technology to share patient health-related information in a secure manner at a level unachievable with a paper record. PKI will play a vital part in this effort.	The GCPR framework project is being used to support and improve the IHS—VA technological conformance. The IHS Information Technology Architecture (ITA) is designed to support cooperation between IHS and VA. Also, the GCPR framework project is supporting the PKI Pilot project.	Continued an active partnership with Department of Veterans Affairs and Department of Defense in support of developing a government-wide foundation for health care information systems as part of the Government Computer-based Patient Record (GCPR) framework project
Staffing/Organization	The CIO and DIR provide overall leadership for staffing/organization to address the information system functions and services within the IHS.		Awarded a 5-year contract for information technology services to DataCom Sciences, Inc. effective September 29, 2000. Employed staff in Rockville, Albuquerque, and Tucson to perform similar functions previously performed by Uniband. Majority of Uniband staff have been re-employed under the new contract making the transition very easy, resulting in a minimum disruption of work.
Security	Planning, assessment, procurement, implementation, and documentation for the overall improvement of security pursuant to Federal legislation, directives, and policies.	The CIO and DIR provide overall leadership for IT security activities and services across the IHS.	(1) IHS conducted the agency's Security Certification Meeting in Albuquerque in November. (2) Development of the agency Critical Infrastructure Protection (CIP) Plan completed. (3) Policy requirements identified to establish policy foundation to support compliance with security requirements and current legis-

IHS National Project Status Sheet

Title	Project Description	Process Approach	Status
			lation (4) CIP briefings presented to leadership bodies including NCEO, TSGAC, NIHB, ISAC, ISC, etc.
Policy Development	Policy development is required by Federal legislation, directives, and policies.	The DIR follows established IHS policy and procedure in the development of IT-specific directives.	(1) Regular meetings and conference call held with ISAC to provide I/T/U partnership in policy, planning, and budget process. (2) Limited Personal Use of IT Resources – DIR revised the Circular according to new HHS policy on the same subject and is resubmitting it for the IHS Director's approval. (3) ISAC Circular-waiting for the IHS Director's signature on the final document. (4) Information Services Manual Chapter – DIR developed an outline of recommended sections (5) Coordinated agency-wide review of 12 major HHS IT policy issuances approved by the Secretary, ASMB, on January 8, 2001. The CIO distributed these policies agency-wide.
Budgeting	Overall participation in and support of the Federal budgeting process.	The DIR is an active member of the Budget Formulation Team and participates in all aspects of development of the IHS budget.	(1) The DIR continues to refine FY2002 budget documents to be included in the President's budget. This includes the IT Exhibit 53-IT Investment Portfolio, the OMB IT Performance Table, updated 300Bs, etc. (2) The CIO represents the agency at monthly HHS CIO Council meetings and receives information on the information technology budget activities occurring within the Department.