August 8, 2002

MEMORANDUM TO: Stuart Reiter
Chief Information Officer
/RA/

FROM: Michael L. Springer, Director
Office of Administration

SUBJECT: CAPITAL PLANNING AND INVESTMENT CONTROL FOR INTEGRATED PERSONNEL SECURITY SYSTEMS (IPSS) PROJECT

The following is in response to your memorandum, dated July 18, 2002, regarding "Capital Planning and Investment Control for Integrated Personnel Security System (IPSS) Project."

The IPSS Business Case in ADAMS is not the latest version of this document. A later version is attached that was reviewed and approved by the CIO Business Case Review Panel. This version has been updated to address the four questions reflected in your memorandum. Please replace the version in ADAMS with this current Business Case. In addition, we agree that the IPSS should be considered a major application and this is reflected in the attached business case.

If you have any questions, please contact Cheryl Stone, of my staff. She may be reached at (301) 415-7404.

Attachment:
IPSS Business Case

MEMORANDUM TO: Stuart Reiter — August 8, 2002
Chief Information Officer
/RA/

FROM: Michael L. Springer, Director
Office of Administration

SUBJECT: CAPITAL PLANNING AND INVESTMENT CONTROL FOR INTEGRATED PERSONNEL SECURITY SYSTEMS (IPSS) PROJECT

The following is in response to your memorandum, dated July 18, 2002, regarding “Capital Planning and Investment Control for Integrated Personnel Security System (IPSS) Project.”

The IPSS Business Case in ADAMS is not the latest version of this document. A later version is attached that was reviewed and approved by the CIO Business Case Review Panel. This version has been updated to address the four questions reflected in your memorandum. Please replace the version in ADAMS with this current Business Case. In addition, we agree that the IPSS should be considered a major application and this is reflected in the attached business case.

If you have any questions, please contact Cheryl Stone, of my staff. She may be reached at (301) 415-7404.

Attachment:
IPSS Business Case

DISTRIBUTION:
DFS R/F (02-0047)
ADM R/F
G. Mathews, OCIO
M. L. Springer, ADM
C. M. Stone, SB

Document Name: CPICIPSSresponse2.wpd
ADAMS Accession No.: **ML022200477**

To receive a copy of this document, indicate in the box: "C" = Copy without attachment/enclosures "E" = Copy with attachments/enclosures "N = No copy

OFFICE	SB		DFS		ADM					
NAME	CMStone		TOMartin		MLSpringer					
DATE	08/06/02		08/08/02		08/08/02					

OFFICIAL RECORD COPY

This document should be placed in ADAMS:
This document should be made available to the PUBLIC: ___TOM___ 08/08/02
This document is NON-SENSITIVE: (Initials) (Date)

August 5, 2002

Business Case for Integrated Personnel Security System (IPSS)
Cost/Benefit/Risk Analysis

REQUIREMENTS IDENTIFICATION AND DEFINITION

Mission Need

The Division of Facilities and Security (DFS) plans, develops, establishes, and administers policies, standards, regulations, and procedures for the overall NRC security program. The Personnel Security (PERSEC) program is a significant part of the overall security program and strategy. The Atomic Energy Act of 1954 requires that all NRC employees have a security clearance. The PERSEC function authorizes access to NRC information, facilities, and certain quantities of strategic nuclear material consistent with National guidelines. The NRC's PERSEC program retains personnel security and database files on more than 10,000 persons. The automated portion of these files is referred to as the PERSEC Modules.

Objective

The objective of this project is to develop an efficient, accurate, and reliable system to replace the current PERSEC Modules software.

The new system would track personnel security processing activities related to:
- the granting of an NRC employment clearance and access authorization (security clearance),
- access to sensitive information technology systems,
- unescorted contractor access to NRC facilities, and
- due process procedures (denial, revocation, suspension and termination of clearance or access authorization).

It would also provide:
- general reporting capabilities,
- a "tickler" system to alert staff when follow-up action is required on clearance matters,
- an internal checking capability to provide data consistency and verification,
- confidentiality and authentication of data, and
- for tracking and recording drug testing functions.

The system would promote more efficient data sharing by consolidating personnel security activities into one integrated system.

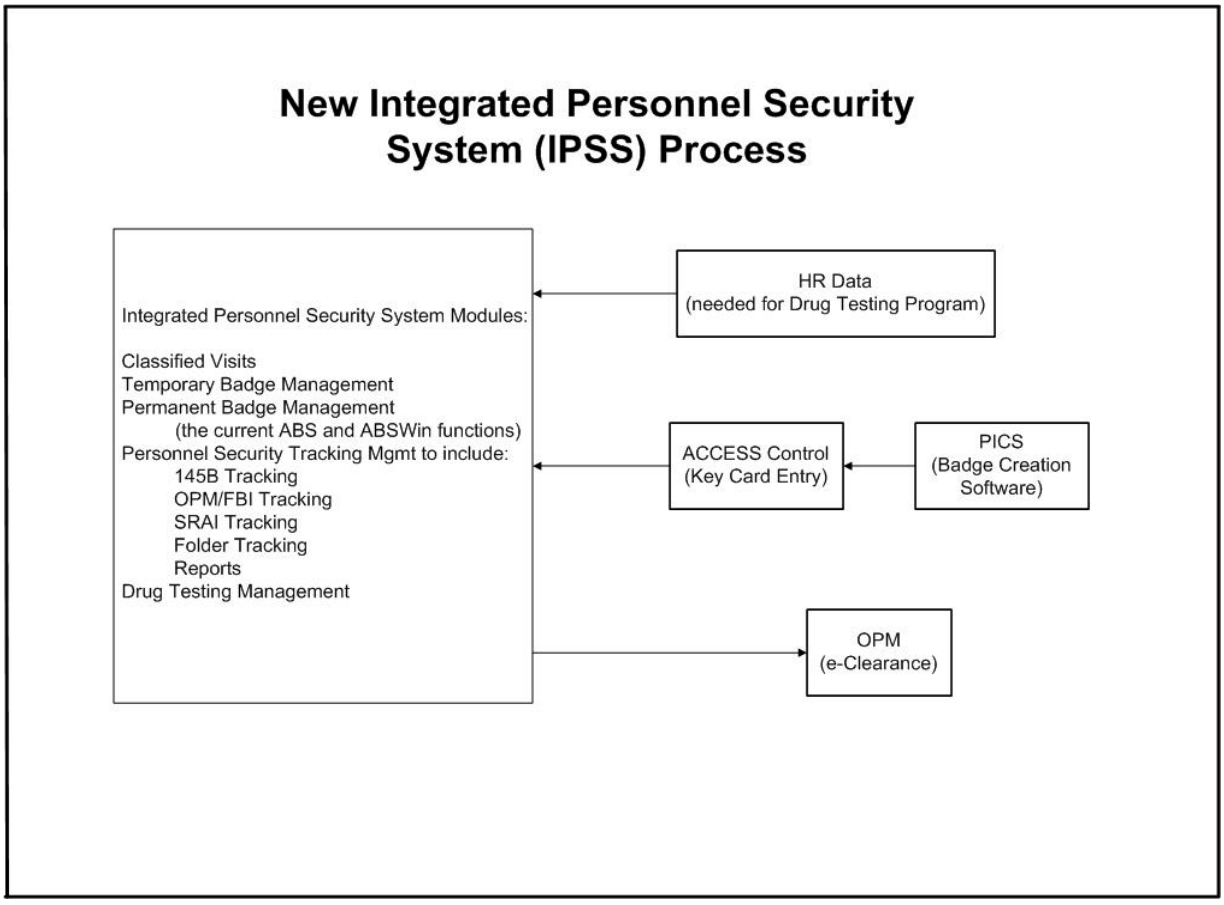
Information Management Problem

The PERSEC Modules, the Classified Visit System, and the Automated Badging System (ABS/ABSWIN) have been used since 1991 to track badging and personnel security processing activities. These applications are antiquated, inefficient, and difficult to provide maintenance support or updates to the software. In addition these applications will not be able to execute in the future when the agency uses newer operating systems on agency desktops. See Attachments 1 and 2 for a detailed list of deficiencies of these current systems and Attachment 3 for system requirements.

Scope

The scope of the project is to develop, deploy, and transition to support an efficient, accurate and reliable system to replace the PERSEC Module. There are some utilities used with the badging system which will be constructed in this application development to simplify use of the software and provide a verification check of data contained in the commercial badging system. The new system would track personnel security processing activities related to:

- the adjudication status of an NRC employment clearance and access authorization (security clearance),
- access to sensitive information technology systems,
- unescorted contractor access to NRC facilities,
- due process procedures (denial, revocation, suspension and termination of clearance or access authorization).
- drug testing dates results



The new system will also serve as an interface between badging and clearance records and provide an automated means for reconciliation between badging and clearance records. The NRC guards will be given privileges to access a section of the system providing them the ability to permit access to NRC facilities, ensuring that the badge issued is consistent with the clearance/access approval level requested. The system will also provide the means to receive alerts on individuals who should be denied entry due to security concerns. The system will provide the capability to record and track all NRC drug testing related activities in addition to providing random drug testing reports.

Stakeholders

Stakeholders for this project are all staff, contractor, and licensee personnel whose information is captured in these systems. Most impacted by the routine use of these systems are ADM/DFS/PERSEC and ADM/DFS/PSB employees. The new system will be available to PERSEC and PSB staff who process, track or manage personnel security data and badging data. Additionally, the NRC guards would use certain data fields from the system to confirm the need for continued access, to verify the identity of employees who lost or forgot their badge, to issue temporary badges as needed, and receive alerts on individuals who should be denied entry due to security concerns. Portions of this data may also be available to other NRC organizational components (e.g., OIG, OGC) on a need-to-know basis after being approved by the Division Director of DFS.

Benchmarking/Redesign Review

PERSEC staff have explored many possibilities for a new system, including evaluating similar systems at other federal agencies (NSA and DOD) and exploring the feasibility of the Interagency Agreement with Census Bureau development approach. One of the government agencies contacted utilized a software package that centralized the Personnel Security and Badging System. One of the other agency's used a database, had no badging system, and did not have the capability to capture enough functions for our use. The results of our Requirements/Market survey is reflected in the "Alternatives" section of this document. The Requirements/Market survey document will be used if we select the approach using the Interagency Agreement with Census Bureau resources or contracted to have the system developed and deployed under CISSCO II. We have attached the Requirements Document and included it as attachment 3.

Data, Functional, and Infrastructure Requirements

Regardless of the option chosen, there is anticipated only a minimal impact on the agency infrastructure. The operational platform and software programming language for the system development will decided by the Project Officer with technical guidance obtained by the implementing contractor in concert with the technical OCIO leads from Infrastructure and Applications Development. It is anticipated that the application will be installed on a new server; however, it will be decided as part of the development and security review process. The Security Branch staff will manually add and delete individuals/user accounts to the database.

Interface with Other Systems

All functions will be contained in one integrated system. An interface with PeopleSoft Human Resources system data will be required to supply basic personal identity information for NRC employees only. System backup will be routine and automatic using existing agency processes.

The present PERSEC module system provides data, along with images of staff, to create the pages used by the ABSWIN system executed by NRC guards to control access to NRC facilities. In addition, it ensures that badges issued are consistent with the clearance/access approval level, and receives alerts on individuals who should be denied entry due to security concerns. The new system will be a fully integrated system.

Potential Solutions
See Alternatives

COST/BENEFITS/RISK ANALYSIS

Summary
The objective of this project is to develop an efficient, comprehensive, interroperable, accurate and reliable system to replace the PERSEC Module system. Using Alternative 3 will provide, through specific SOW, that we have programmers knowledgeable in security regulations, issues and policies in addition to the new government wide personnel security related initiatives. This is part of the new administration's e-government and homeland security initiatives. This system directly supports the E-Clearance Initiative which has been mandated by OMB to be operational by 31 December 2002.

E-clearance is one of the e-government initiatives. It is composed of 3 components, 1 - Electronic Questionnaire for Investigations processing (e-QIP), 2 - cross-agency clearance Verification System and - is to image investigative records. The e-QIP and the image will require a single data filed and the CVS requires us to produce a flat file all of which will have a minor impact on our system.

Objectives
The objectives for this project are as follows:

- track all personnel security processing activities related to the approval or denial of an employment clearance and access authorization,
- track both interim and final access to sensitive information technology systems;
- track unescorted contractor access to NRC facilities;
- track due process procedures (denial, revocation, suspension and termination of employment clearance or access authorization);
- provide reporting capabilities;
- provide a "tickler" system to alert staff when follow-up action is required;
- provide data input along with the images of staff to serve as a badging verification system;
- provide for data consistency, confidentiality, and authentication;

- promote efficient data sharing by consolidating personnel security activities into one integrated system.

- track drug testing activities;

- provide random selection and tracking of drug program participants; and

- provide multiple drug testing reports.

Background

The Administration Activity identified in the Performance Plan includes responsibility for personnel and physical security functions, as mandated by the Atomic Energy Act of 1954, as amended. Personnel security functions include requesting and adjudicating personnel security investigations for NRC employees and contractors requiring a security clearance; for NRC licensees requiring a clearance or special nuclear material access authorization under 10 CFR Parts 11 and 25; and for NRC contractors requiring access to sensitive information technology systems under the NRC Contractor Access Program. Physical security functions include protecting NRC personnel and property by ensuring that the NRC badge issued is consistent with the clearance/access approval level, confirming the need for continued access by contractor staff, and receiving alerts on individuals who should be barred from entry due to security concerns.

Since 1991, the PERSEC Module software has been used to track personnel security processing activities. This is a DOS-based system (written in Clipper), consisting of eight distinct modules. These modules are described in detail in Appendix 1.

The function of the Permanent Badge Management in the new system will perform those functions currently done by the Automated Badging System (ABS) and ABSWIN. ABS serves as an interface between badging and clearance records and provides badge tracking accountability (e.g., to ensure that the badge issued is consistent with the clearance level); ABSWIN contains the badging records in ABS plus the photo images from PICS (badge manufacturing system).

Assumptions

The work plan is based on the following assumptions:

1. Use current infrastructure and operating system

2. The Clearance Verification System portion of the e-clearance will require a flat file with no active interface with only minor impact on the system.

3. Future enhancements in the DHA requirements document will have minimal impact on our system.

4. Specifics of the transmission of output file to OPM have been defined by OPM and may have an impact on the infrastructure as e-government initiatives become further defined.

5. Back ups managed by current infrastructure.

6. Anticipate no impact on current infrastructure

Description of Alternatives

Alternative 1: Retain current method of tracking all personnel security processing systems. This system is unsupportable because it is written in Clipper and dBaseIII and needs to be converted to a Windows-based Operating System so that it will work under Windows NT. Furthermore, this application is likely to become inoperable as the infrastructure upgrades to newer operating systems and hardware, which are not compatible with the legacy DOS applications. This alternative is not recommended and will not be adopted.

Alternative 2: Explore the feasibility of Interagency Agreement with Census Bureau development of a new software application. If written via the Interagency Agreement with Census Bureau, we intend to use the agency standard off-the-shelf software and the existing infrastructure support. If this alternative is adopted documentation to the level called for in SDLCM may be an issue and could slow the certification and accreditation by OCIO and D/DFS of the system. It is also very important to ADMIN that this system take advantage of the latest security knowledge available in the field. In addition, this development is part of the new administration's e-government and homeland security initiative. This system directly supports the E-Clearance Initiative which has been mandated by OMB to be operational by 31 December 2002. This alternative is not recommended.

Alternative 3: Use a contractor to build the system to PERSEC's requirements. This would most likely be accomplished using the CISSCO II contract vehicle. This is recommended as the most viable option to compete this project. Using Alternative 3 will provide, through specific SOW requirement, that we have input from contractors who are knowledgeable in security regulations, issues and policies in addition to the new government wide personnel security related initiatives. This is part of the new administration's e-government and homeland security initiatives. This system directly supports the E-Clearance Initiative which has been mandated by OMB to be operational by 31 December 2002.

Summary Table Comparing Non-recurring and Recurring Costs of Alternatives

(K = 000, FTE rounder to the nearest whole number)

Alt. 1 Status Quo	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	TOTAL
Non-recurring costs $ FTE	 0 N/A	See Note 200K N/A	 0 N/A	 0 N/A	 0 N/A	 0 N/A	 200K N/A

Recurring costs $ FTE	45K 2	45K 2	45K 2	45K 2	45K 2	45K 2	270K 12
Total $ FTE	45K 2	245K 2	45K 2	45K 2	45K 2	45K 2	470K 12

Note: There will be a major expense required when we transition to Windows 2000 to force compatibility with a new desktop operating system and infrastructure.

Alt. 2 IA with Census Bureau	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	TOTAL
Non-recurring costs $ FTE	160K (see note) 2.5						160K 2.5
Recurring costs $ FTE		45K See note 1.5	45K See note 1	45K See note 0.5	45K See note 0.5	45K See note 0.5	225K 4
Total $ FTE	160K 2.5	45K 1.5	45K 1	45K 0.5	45K 0.5	45K 0.5	385K 6.5

Note: $100K for 1/2 year of Interagency Agreement and $60K for additional documentation
Stuart Lynn, from OCIO, will count as 0.5 FTE due to Systems Analyst activities.

Alt. 3 Contract Out	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	TOTAL
Non-recurring costs $ FTE	180K 2	See note	See note				180K 2
Recurring costs $ FTE	0	45K 1	45K 1	45K 0.5	45K 0.5	45K 0.5	225K 3.5
Total $ FTE	180K 2	45K 1	45K 1	45K 0.5	45K 0.5	45K 0.5	405K 5.5

Summary Table Comparing Benefits of Alternatives

Category of Benefits of Alternatives	**Score (1 = high benefit, 5 = low benefit)**		
	Alt 1: (Status Quo)	**Alt 2: (Interagency Agreement with Census Bureau)**	**Alt 3: (KTR)**
Quantitative			
FTEs saved (identify specific office) ADM	None	0.5	0.5
Monetary savings	No savings	1	1
Quantified performance/service improvements	None	1	1
Other Quantifiable benefits	None		
Non-Quantitative (illustrative examples shown below)			
Improved customer/user satisfaction	None	2	2
Improved data quality and consistency	None	2	2
Improved access to information by staff, licensees, or the public	None	1	1
Better information for management decision-making	None	1	1

Summary Table Comparing Risks of Alternatives

Category of Risks of Alternatives	**Score (1 = low risk, 5 = high risk)**		
	Alt 1: (Status Quo)	**Alt 2: (Interagency Agreement with Census Bureau)**	**Alt 3: (KTR)**
Volatility of Requirements - requirements may change based on e-government initiatives - Alternative 1 represents the status quo with no change to PERSEC modules. Additional upgrade applications may not be supported due to outdated software.	2	2	2
Scope of Proposed Project - Scope is relatively small and only involves ADM.	NA	2	2
Technical Risk - Alternative 1 is archaic. Alternative 2 and 3 pose little risk in development because of the simplicity of design	NA	1	1
Team Consensus - Alternative 1 is seen as slow and cumbersome. Focus group representing ADM provided input on the requirements for Alternative 3 and is supportive of the project because it will be designed to be more user-friendly, has data integrity checks and will have thorough documentation in accordance with the NRC SDLCMM. Alternative 2 is a 2 because there is a lower knowledge of the Federal Government's regulations and e-initiatives as well as a weaker knowledge of the SDLCM Methodology and its required documentation.	5	2	1
Resource Commitment - Funding has been estimated and budgeted by management.	1	1	1

Potential Resistence - Alternative 1 would be viewed as negative by the PERSEC staff because it is becoming obsolete and difficult to use. Alternative 2 is a 2 because there is a lower knowledge of the Federal Government's regulations and e-initiatives as well as a weaker knowledge of the SDLCM Methodology and its required documentation.	5	2	1
Procurement Risk/Vendor - No new contracts or equipment will be required for Alternative 1. Alternatives 3 offers more long term support and support throughout the development of the project.	1	2	1
Sponsor Organization's IT Project Management Experience - The IT coordinator for ADM has significant technical experience with projects of this type. The project manager has significant experience in the provision of administrative services.	1	1	1
TOTALS	15	13	10

(UNDISCOUNTED DOLLARS AND FTE FOR FISCAL YEARS 2002-2007)
(K = 000, FTE rounded to the nearest whole number)

Expense Category	Alt. 1		Alt. 2		Alt. 3	
	$	FTE	$	FTE	$	FTE
1. Non-Recurring, One Time Cost for Development	200K	0	160K	2.5	180K	2
2. 5 Yr Recurring Cost (HW, SW, systems-related)	270K	12	225K	4	225K	3.5
3. Total Cost (Sum of Rows 1 & 2)	470K	12	385K	6.5	405K	5.5

Discussion of the Return on Investment of the Alternatives Based on the Summary Tables for the Costs, Benefits, and Risks

Using Alternative 3 will have the best return for the investment for this IPSS. ADM/DFS will have a state-of-the-art system that will be efficient, accurate and reliable in all areas of costs, benefits and risks associated with this project and a system will be compliant with the e-government requirements. Over the long run, the fully documented system code prepared by the CISSCO II vendor will be make changes to this code less expensive to modify. This system

directly supports the E-Clearance Initiative which has been mandated by OMB to be operational by 31 December 2002.

Sensitivity Analysis

The assumptions that were used in the cost analysis were not considered volatile enough to warrant a specific sensitivity analysis. Even in light of the future enhancements defined in the DHA document it will not increase the volatility of this system.

Results (With Sponsor's Recommendation of Alternative and Course of Action)

The project team selects Alternative 3 for the following reasons:

1. Lowest risk for overall project success through development compliant with CIO systems development standards and documentation.

2. Lowest risk for follow on/long term support and maintenance.

3. Greatest benefit derived from contractor knowledge of security regulations and government-wide security initiatives.

4. Increase Commission's security by enhancing the management of security systems.

Appendices

Appendix A - System/Application Description
See DHA System Requirements Document (Attached)

Appendix B - Cost Estimates
The present system is antiquated, using software and programming languages that are no longer generally supported by the agency.

Alternative 2 will be provided under the Bureau of Census Interagency Agreement through FY 2002 at a cost of $160,000 for programming with an additional contractor hired to write the documentation. Recurring costs for Alternative 2 assumes technical support for maintenance and minor modifications. These recurring costs are estimated to be $45,000 per year.

Alternative 3 costs are estimated at $180,000. These costs include programming, software documentation, data conversion, labor and future design interfaces. Recurring costs for Alternative 3 assumes technical support for maintenance and minor modifications. These recurring costs are estimated to be $45,000 per year.

Appendices C and D - Risks and Benefits - Tables are shown above

All alternatives assume that we use the current NRC hardware and infrastructure.

For all other categories under this heading, please see DHA System Requirements Document (Attached)

Benefit Categories for Appendix C

Quantitative

FTE Saved
The System Coordinator currently expends several days per month identifying and correcting data entry errors. With the addition of required system checks, this time is expected to be reduced to approximately one hour.

Monthly exception reports are produced from ABS to identify discrepancies between the clearance record and the badge record and reconciled manually. With the addition of a system "tickler" that alerts users whenever a clearance level changes, this time is expected to be reduced to 1-2 hours per month from 15 hours per month.

With system-generated reports, the time expended creating specialized reports is expected to be reduced to 4-5 hours per month from 40 hours per month.

PERSEC staff will be able to generate their own data and statistics needed to perform their functions, rather than relying on the IT Coordinator to produce this information. Two days of staff time will be saved per month.

Monetary Savings
There will be cost savings in terms of staff time and development of the system to be realized by adopting either alternative 2 or 3 as opposed to the other Alternatives. Modifying Alternative 1 is not an option because it will become inoperable as the infrastructure upgrades are made to newer operating systems and hardware, which will not be compatible with the legacy DOS applications.

Quantifiable Performance/Service Improvements
The new system will give us the functionality to obtain data to use for long-range planning to assess workload and budget projections and investigative costs. The new system will also provide improved data integrity, tracking of personnel security data, and enhanced reporting capabilities. This project is necessary to ensure that NRC's personnel security program is in compliance with federal regulations. Alternative 3 or 4 shall reduce the time required to resolve discrepancies between the clearance record and the badge record from 1-2 days per month to 1-2 hours per month. It is also expected to reduce the time required to produce system-generated reports from several days per month to 2-3 hours per month, and to reduce the time expended correcting security clearance data records from several days per month to 2 hours per month. In addition, it will provide the means to provide clearance data to OPM as required by E.O. 10450 and it will have the ability to provide real-time clearance data to other agencies, upon request.

Other Quantifiable Benefits
None

Non-Quantitative

Improved Customer/User Satisfaction
The new system will provide the method for compliance with Executive Order 12968, in that a record of all actions will be recorded and tracked - and will significantly simplify the process of sharing personnel security information with other agencies.

Improved Data Quality and Consistency
The new system will provide significant improved data quality and consistency just in regard to denial of service and corrupted data. At present, with the use of the Clipper program, it would take a long time to learn the Clipper language because it is not widely known. New and improved programming languages have taken the place of Clipper that respond better to the Novell platform. It is difficult to find an expert in Clipper programming.

The data check functionality built into the new system will provide a high level of data integrity and confidentiality. Because this system will contain highly sensitive privacy and personal data, it is critical to ensure its availability, confidentiality and integrity.

Improved Access to Information by Staff, Licensees, or the Public
The system would promote more efficient data sharing by consolidating personnel security activities into one integrated system as opposed to 8 stand-alone modules. This will eliminate the need to enter data multiple times and will allow us the ability to provide a quicker response to our customers.

Better Information for Management Decision-making
See above response.

Security Benefits
The elimination of data corruption will ensure bared individuals will not have access to the buildings. It will improve the management of security throughout the agency.

PROJECT MANAGEMENT PLAN

Non-recurring Cost/Project Schedule/Spending Plan

The chart below describes the anticipated steps of the project and the approximate costs incurred at these steps. This material will be formalized when the project starts and the Project Plan is delivered.

Action	**Estimated Cost**	**Estimated Days**
Requirements Analysis	20K	Project start +5 days
Acquire Support Resources	5K	Project start +25 days
Analyze/Design/Verify Functional Requirements	10K	Project start +55 days
Business Continuity Plan	10K	Project start + 65 days
Plan Solution Integration	15K	Project start + 85 days
Engineer Solution	60K	Project start + 145 days
System Testing	10K	Project start + 175 days
Production System Integration	5K	Project start + 185 days
Finalize Documentation	15K	Project start + 210 days
Conduct Training	10K	Project start + 215 days
System Acceptance Testing	15K	Project start + 230 days
Certification & Accreditation	5K	Project start + 235 days
System Deployment	5k	Project start + 240 days
System O&M Transition	5k	Project start + 245 days

Recurring cost elements for alternative 3 (including 5 years of operation)

Action	Estimated Cost
Hardware and commercial software licenses and maintenance	0
Application operations and maintenance support	225K
Infrastructure operations and maintenance support	0
Data entry/update	4 FTE (for 5 years)

Cost of maintaining interfaces to other applications	0
Cost of adapting any custom code to new releases/versions of COTS	0
Training for new COTS releases/versions	NA

Staffing Plan

The following Roles and Responsibilities have been named for the conduct of this project:

The executive sponsor will be Cheryl Stone

The Project Officer and Technical Lead for this project will be Karen Cudd. (She will contribute 65% of her time to this project.)

It is anticipated that John Davis, from OCIO, will be consulted as needed (less than 5%)

The Project Functional Leads are Cynthia Harbaugh, Sandra Schoenmann, Patricia Smith and Christine Secor who will each contribute 40% of their time.

The OCIO Project Technical Advisor will be Stuart Lynn who will contribute 15% of his time to support the development.

Contractor resources will be dedicated to this effort.

Outcome Oriented Performance Goals and Associated Metrics That Can Be Used To Objectively Measure the Success of the Project

The following output measures contained in ADM's FY 2001-2004 Operating Plans and NRC's FY 2002 Performance Plan will be used to measure the success of this project.

Measure	Current	Target
Percentage of report requests satisfied	10%	90%
Percentage of equipment service calls corrected under initial response	None	90%
Percentage of data errors	25%	0%
Percentage of data-integrity checks included in application where applicable	0%	100%

Data entry time for employment clearance/reinvestigations will be completed within 15 minutes.	0%	100%

Statement of conformance with the agency's standards for the SDLCM, IT architecture, infrastructure, data, and network standards

The PERSEC system, under Alternative 3, will conform to the software standards set by the Office of the Chief Information Officer as well as the agency's standards for the SDLCM methodology.

A statement as to whether the proposed IT investment would or would not result in shared benefits or costs with other Federal agencies or State or local governments. (If there would be such results, an estimate or description of the benefits or costs should be included with the statement.)

Using Alternative 3 would result in shared benefits with other Federal Agencies for reciprocity of clearances, namely the Federal Bureau of Investigations National Crime Information Center 2000 system and OPM's guidance on e-clearance initiatives of the new Administration and homeland security. This system directly supports the E-Clearance Initiative which has been mandated by OMB to be operational by 31 December 2002. It will also provide a quicker response to our customers with more complete data.

System Security

We have addressed Government Information System Reform Act (GISRA) and this system does fall under the definition of a major system. We have addressed the Government Information System Reform Act (GISRA) legislation and discussed this with the CIO Security Executive, Dan Galik, and we have categorized this system as a major application. The Business Continuity planning will be addressed early and throughout the project resulting in Certification and Accreditation prior to going into production.

Acquisition Approach
This requirements package will be bid out according to policy and procedures under CISSCO II.

Acquisition Approval

_____ Date:_____

_____ Date: _____

Appendix I

Description of PERSEC Modules Systems

Main Program Menu

1. Preprocessing Module - Tracks activities associated with the 145b program, power plant access by employees and contractors, unescorted building access by contractors and interim IT approval for contractors requiring access to sensitive information systems and data.

2. Processing Module - Tracks OPM/FBI investigative requests and clearance/final access approval data for employees, contractors and licensees requiring an initial or upgraded clearance, licensees requiring a Special Nuclear Material access authorization, and contractors requiring access to sensitive information systems and data.

3. Reinvestigation Module - Tracks OPM/FBI reinvestigation requests and clearance/access approval continuation data for employees, contractors and licensees with a clearance, for licensees with a Special Nuclear Material access authorization, and for contractors with access to sensitive information systems and data.

4. SRAI Module - Tracks the processing of cases containing adverse information affecting the eligibility for a clearance, Special Nuclear Material access authorization or access to sensitive information systems and data.

5. Folder Module - Tracks module location of personnel security records.

6. Reports Module - Produces reports of pending and completed records in the Preprocessing, Processing and Reinvestigation Modules.

7. Certification Module - Tracks and verifies OPM/FBI investigative charges.

8. SRAI Reports - Produces reports of cases containing adverse information.

The ABS serves as an interface between badging and clearance records and provides badge tracking accountability (e.g., to ensure that badge issued is consistent with clearance level); ABSWIN contains the badging records in ABS plus the photo images from PICS (badge manufacturing system) - following three systems will be under the interface umbrella, but do not involve requests for services. These systems are for ADM staff and management information only and are not flow charted. The tracking of Trans Union Reports; OPM Costs and FBI Costs will also be included.

Attachment 1

PERSEC MODULES - SYSTEM DEFICIENCIES

1. Non-compliance with Federal regulations - Executive Order 12968, "Access to Classified Information," mandated a uniform Federal personnel security program and standardized the adjudicative guidelines, investigations and reinvestigations. The system does not capture the required data (e.g., adjudicative guideline criteria). It also does not show a clearance history, which is required for reciprocity between agencies and for further actions within NRC (e.g., upgrades).

2. Application to become obsolete - This is a DOS-based system written in Clipper, which is no longer used for new applications. Furthermore, this application is likely to become inoperable as the infrastructure upgrades to newer operating systems and hardware, which are not compatible with the legacy DOS applications. This recently occurred with the FedReg system, another DOS-based application in ADM. The user's machine was "refreshed" with a Pentium P3 (500 megahertz) machine, which is too fast for that application; it will not run on that machine.

3. Inability to multi-task - Because opening a module utilizes 100% of resources, it is necessary to close one module before opening another. This limits the user to single tasking, which is very inefficient since it is often necessary to obtain data from two or more modules.

4. Slow response time - Accessing the Modules can be very slow; running a simple report can exceed 30 minutes.

5. Inability to access modules - If a user has left the cursor on the "find" screen of a module, other users are often unable to access any of the modules.

6. Frequent downtime - Inaccessible module(s) due to corrupted indices or data. Resolution of this problem is accomplished with great difficulty (see #14) and must generally wait until the overnight reindexing program is run.

7. Redundant data entry - Many data fields have to be entered twice. For example, the NCIC and credit data fields are entered in the Preprocessing Module. When the investigative data is entered in the Processing Module, this data must be reentered. Furthermore, all data has to be entered in the Reinvestigation Module when an individual is due for reinvestigation, despite already having an active clearance record in the Processing Module.

8. Inadequate reporting - Although we began using the PERSEC Modules in 1991, we continued to enter clearance data into DOE's CPCI system as well. When we discontinued using CPCI for data entry in 1996, we lost essential management information data that had been obtained from CPCI reports. There are no reports for this data in the Reports Module. This has resulted in significant time expended to create the queries and ad hoc reports needed to capture and retrieve data. For example, there are no reports to provide active record counts, including active records by employer or by clearance, investigations sent to OPM or investigations sent to OPM but not certified. This vital data is often requested by both

DFS/ADM management as well as other NRC offices. It is also needed for performance output measures and reports to Congress (e.g., Synar report). There are also no reports to assist in performing routine PERSEC activities, such as determining the monthly obligations for security investigations, adjudicative decisions and NCIC usage.

9. Inaccurate reports - Occasionally a record will appear on a pending report for no apparent reason. For example, a record that has been granted final access approval will appear on the pending access approval report. This problem can only be resolved by deleting the record entirely (from the name database as well) and then reentering all of the data.

10. Update problems - Occasionally, after a record is updated and saved, these updates are not reflected when the user later accesses the record.

11. Cumbersome and confusing data entry screens - As a result of the multitude of screens, data is sometimes entered in the wrong one, e.g., a building access contractor data is erroneously entered in the AIS contractor section. Numerous discrepancies of this nature are discovered during quality control checks and in performing comparisons of clearance data against NRC payroll data. To resolve these problems, the entire record must be deleted from the module and then all data reentered.

12. Incompatibility with Payroll file - DFS receives an MSAccess table of active employees to compare with the name database to ensure data integrity of LAN data. To accomplish the comparison, it is necessary to convert the Access table to a dbf file and then compare the two databases in Reportwriter.

13. Insufficient system checks - Many fields lack necessary system checks, resulting in the entry of erroneous data. Although some checks have been added over the years, many more are required to ensure data integrity (e.g., limits on year of termination or grants, employer codes requiring a numerical prefix, limiting entry of certain employer codes based on type of action) .

14. Inability to reindex the databases - A system reindex is often needed to alleviate the problem described in #6. A reindex can only be performed if all users are off the system. This is very difficult to accomplish because there are always users accessing ABS (a submodule), including the NRC guards and approximately 30 other NRC personnel throughout the agency.

15. Backup problems - Due to the number of users on the system (accessing ABS), it has been impossible to obtain a complete backup of all databases.

16. Problem deleting “bad” records from databases or performing other system maintenance - When a record has been entered twice for the same person (w/different SSN’s), or an individual has been entered in the wrong screen (see problem #11), it must be marked for deletion and removed from the database. This can only be performed when all users are off the system. Like backup and reindexing, this has been impossible to accomplish. PERSEC has been coordinating with OCIO since late fall 1999 to arrange for all users to be out of the system for a period of time each evening, so that backup and system maintenance tasks can be accomplished.

17. Dependency on one PERSEC employee to obtain all reports/statistics - Much of PERSEC's reporting/statistical needs are not met with the reports available from the Modules (see #8), so special reports must be created in Reportwriter and dBASE. No other PERSEC staff member is knowledgeable of these two software programs (courses are not even offered for these outdated programs), nor do they possess an adequate understanding and familiarity of the PERSEC Modules.

18. Overnight reindexing problems - For no apparent reason, the overnight reindexing program (Time Target software) fails to run approximately half the time. Furthermore, the program is not serviceable by OCIO contractors, so problems or questions must be directed to the software manufacturer. This has proven to be time-limited (the company is in California) and generally unsuccessful.

19. Incompatibility with other agency systems - The SSN contains dashes, which is incompatible with other systems. For example, when uploading PERSEC LAN data to OPM's Clearance Verification System (CVS), it is necessary to manually delete all dashes from both the processing and name databases in order to conform with CVS requirements.

20. Multiple entry of user ID and password - It is necessary to enter a user ID and password each time a user accesses one of the eight modules. This is cumbersome and time-consuming since it is often necessary to go from module to module to check the status of a particular record (e.g., access the Processing Module for grant date and then the Reinvestigation Module for latest reinvestigation data).

21. No tracking system - There is no "tickler" system to flag issue cases, such as identifying individuals who require recontact in a specific time frame to resolve ongoing security concerns.

22. Non-user friendly - Entering/updating preprocessing and investigative data requires access, depending on the type of action, to 16 separate screens within 3 distinct modules.

23. Obsolete fields - A number of fields in the PERSEC Modules are now obsolete and their existence causes confusion, particularly for new contractor processing staff.

Attachment 2

ABS/ABSWIN - SYSTEM DEFICIENCIES

1. Inability to access ABSWIN - This occurs at least several times each month and is generally linked to the failure of the overnight reindex function. When this occurs, the guards must resort to searching an outdated hard-copy printout to verify a clearance level.

2. Index problems - Several of the ABS reports frequently mis-sort due to index problems. Resolving this problem requires manual comparisons of data and correcting the data using dBASE and Reportwriter.

3. Insufficient system checks - There is no system check to preclude a double entry in ABS. When such an entry is made, the record becomes inaccessible by name and can only be accessed by SSN. Since ABSWIN can only be queried by name and not by SSN, the record may be unavailable to the guards.

4. Limited query capability - ABSWIN can only be queried by name. In addition to limiting the guards search capability, the inability to also conduct searches by SSN results in the complete inaccessibility of the records cited in #3.

5. Obsolete fields - A number of fields in ABS are now obsolete.