

GAO

Report to the Commissioner of the U.S.
Customs Service

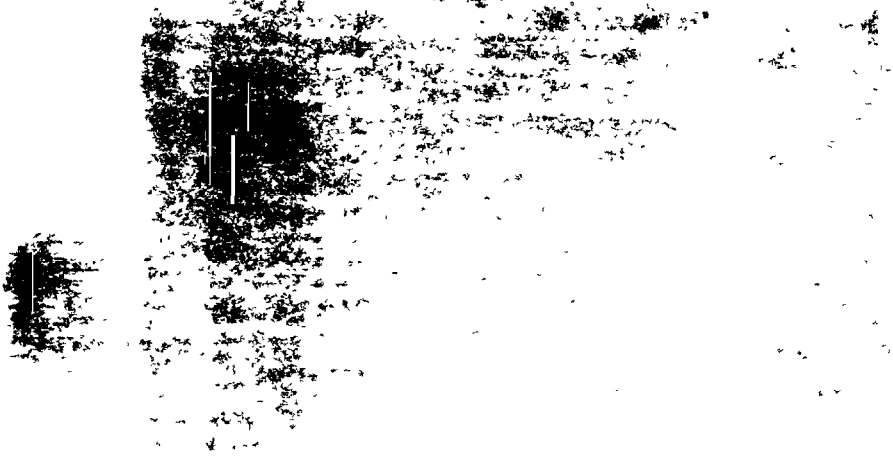
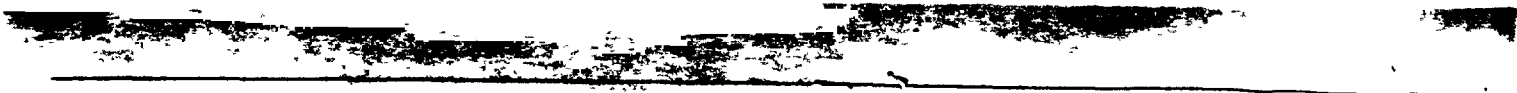
February 1987

SYSTEM INTEGRITY

Stronger Controls Needed for Customs' Automated Commercial System



038160





Information Management and
Technology Division

B-224062

February 10, 1987

The Honorable William von Raab
Commissioner of Customs
Department of the Treasury

Dear Mr von Raab:

We reviewed the U.S. Customs Service's Automated Commercial System (ACS) because it is one of Customs' mission-critical computer systems and because we wanted to determine if this system had any weaknesses that could affect its integrity or reliability. ACS is being used to help staff identify and examine imported goods and collect duties owed. In addition, ACS will provide the Department of Commerce with current import data used for computing economic statistics and in recommending international trade policy.

We found that Customs has not

- established adequate controls to prevent employees from unwarranted access to ACS functions not required to perform their specific jobs,
- documented clearly enough how ACS operates so that modifications can be made with minimal time and effort and without introducing errors, and
- developed formal test plans for use in testing programs to ensure that software is produced that will meet user needs while maintaining system integrity.

Because Customs will increasingly rely on ACS to support its enforcement activities and to collect billions of dollars in revenue, these deficiencies need to be corrected as soon as possible.

Objective, Scope, and Methodology

Our objective was to determine if ACS had any weaknesses that could affect its integrity or reliability. We conducted our review at Customs' headquarters in Washington, D.C.; the data processing center in Franconia, Virginia; the New York region, including the Seaport area, the Pacific region, including the Los Angeles District and the ports of Los Angeles and Otay Mesa, California; Seattle and Blaine, Washington, and the Port of Buffalo, New York. Functional access data from the North Central region was reviewed at Customs' headquarters

We discussed the operation of the system with customhouse brokers,¹ and managers and staff in Customs' operations. Federal regulations and publications and Department of the Treasury and Customs directives were reviewed. Our review was conducted in accordance with generally accepted government auditing standards. We conducted our work primarily between October 1984 and November 1985, and made follow-up inquiries in September 1986.

The development of security controls for ACS is being reviewed in more depth in another GAO audit;² a report is planned for publication in spring 1987.

ACS Is Critical to Customs' Mission

At the end of fiscal year 1986, over \$56 million had been spent or budgeted for ACS hardware and software development. Customs expects that total life cycle costs for developing and operating ACS will exceed \$2 billion over its expected 10-year life.

In the last decade, Customs has experienced a significant increase in the volume of imported merchandise. For example, during the last 5 years, formal merchandise entries³ have grown from 4.5 million to 6.8 million; duties collected on these entries rose from \$9.1 billion to \$13 billion. The need to process this increased work load faster and with fewer people caused Customs to seek a modern, automated system that could handle all aspects of its commercial processing responsibilities. Customs began planning ACS in fiscal year 1982; hardware and software acquisitions (totaling about \$5.8 million) came the next year. The system began operation with only minimal components, such as revenue accounting, in February 1984. While development of the full system continues, features of the system providing interface with the trade community⁴ and

¹Customhouse brokers act as agents for importers. They are responsible for preparing and filing all necessary import entry documents and paying any duty owed.

²The Chairman, House Committee on Science and Technology, requested this audit of security development activities for ACS and eight other federal systems.

³A formal merchandise entry represents the filing (with the appropriate Customs officer) of all documentation required by Customs' regulations. This documentation is used to assess any duty and to collect statistical data on imported cargo. It is also used to determine if all legal requirements regarding the imported merchandise have been met.

⁴The trade community consists of importers and businesses such as carriers, customhouse brokers and container station operators.

those allowing Customs staff to more efficiently identify high-risk merchandise for inspection are substantially in place. Completion of the total system is scheduled for fiscal year 1987.

ACS is a large, complex, integrated system designed to replace seven individual stand-alone systems. It is also intended to reduce the resources that Customs needs to process its work load. The reduction is to be achieved in three ways. First, redundant data entry from the prior seven, non-integrated systems will be eliminated. Second, an automated interface with the trade community will allow electronic transfer of data to ACS. Third, ACS will use the data from this automated interface to select only high-risk merchandise entries for detailed examination.

Customs Needs to Tighten Access Control to ACS

Office of Management and Budget Circular A-130 (1985), National Bureau of Standards Federal Information Processing Standards publications,⁵ and Customs' own procedures require protection of critical systems such as ACS from unauthorized access, fraud, and abuse.

Customs has implemented two measures—passwords and functional access codes—intended to provide such protection. A password is a sequence of characters that authenticate a user's identity, thereby limiting system access to only authorized employees. Functional access codes allow users to access only certain data and to perform only certain operations on those data. This separates tasks into two or more parts, each of which is performed by different staff members. This separation of duties principle helps to ensure that an individual cannot commit a fraud: it would take two or more employees, acting in collusion, to commit fraud. Although the principle predates automation, it is still a valid control technique in an automated environment.

Early in our work we found that these two controls were not providing adequate protection. The necessary procedures to implement the control of passwords were not being taken; nor was access by individual employees being controlled to ensure that separation of duties was maintained. Customs has since installed a new security system to provide an adequate level of password control. However, granting functional access to individual employees is still inadequately controlled.

⁵Guidelines for Security of Computer Applications, Publication Number 73, National Bureau of Standards (Washington, D C , 1980) and Password Usage, Publication Number 112, National Bureau of Standards (Washington, D C , 1985)

Customs Has Not Controlled Functional Access

Federal computer-security guidelines state that individuals should be authorized access to only the data necessary to perform a job function. This requirement means that individuals' transactions are limited to their assigned duties rather than to a broader, more generic activity (such as merchandise entry or liquidation), as is currently the case.

When ACS became operational in February 1984, it replaced seven separate systems that individually performed discrete portions of merchandise processing. To use ACS, employees had to have access to functional areas equivalent to those they had used in the prior system(s). Consequently, users were given, through a one-time mass conversion, all access codes necessary to perform at least the same functions they had been performing. Individuals, therefore, received access to many ACS functional areas because it is an integrated system, not several stand-alone systems. Accordingly, it became possible for employees to have access to more functional areas than necessary to perform their specific jobs.

To evaluate this, we reviewed access codes granted to 508 employees in the New York and Pacific regions and Los Angeles District Offices. We found that 76—too many to maintain overall system security—had access to functional areas beyond their needs. Of the employees affected,

- 32 had access to parts of ACS not required for their job performance; additionally, 13 of the 32 had access to areas that allowed an individual to handle all aspects of a transaction;
- 43 (current or former employees) had access to ACS functions that should have been deleted because the individuals had either transferred to different positions or had terminated employment; and
- 1 was never granted ACS access but used, with supervisory approval, the access of a previous employee.

To determine if the excessive granting of functional access codes was due solely to the mass conversion, we reviewed subsequent requests for access codes. We analyzed 757 access requests from the two regions—New York and Pacific—in which our audit work was conducted, plus the North Central region, which ACS' Security Administrator selected as typical. These requests covered the nearly 8 months following the mass conversion. Since virtually all the requests were for broad groups of functional access codes, the trend of excessive access authorization, established at the time of mass conversion, was continued.

Customs Needs to Document ACS' Operations

Because ACS is such an important system, it is essential that it be maintained (modified or enhanced) without disturbing its integrity or operation. Systems need modification when errors are detected, when user requirements shift, or when laws and regulations change. The key element in maintaining systems is the availability of documentation, and Customs is not producing all the documentation necessary for system maintenance.

Documentation is the process of stating how an automated system operates. Good documentation should clearly and comprehensively describe what the system does and how. This includes the general interrelationship of the system's components or modules. Documentation also increases the ease and accuracy of computer program and system maintenance.

Federal guidelines for information-processing management underscore the importance of developing systems that can be effectively and efficiently maintained because systems usually represent a considerable investment of resources. The guidelines strongly suggest formal documentation for complex, mission-critical systems such as ACS. Customs also recognizes the importance of system documentation. In a June 23, 1983, presentation to Treasury's System Review Committee, Customs stated that ACS should be completely documented to the standards prescribed and that a mechanism would be available to regulate and document all changes. Customs also stated that quality-assurance reviews would provide an adequate and usable level of documentation for the system to ensure ease of maintenance.

We found, however, that Customs did not document the interrelationships among ACS' 15 distinct modules or functional areas because it placed a higher priority on implementing ACS as quickly as possible. This emphasis grew out of several previous, unsuccessful attempts to redesign its automated support for its commercial regulation and to improve productivity. With the Customs Commissioner's personal involvement and direction, the agency committed itself to placing the first phase of ACS in operation within 8 months of the project's start. Customs officials told us that this ambitious schedule required every available resource directed to the delivery of operational programs. In addition, Customs used a streamlined approach to systems development that does not require certain documentation normally associated with systems development. Therefore, documentation beyond that minimally necessary to

deliver the program (i.e., instructions to the computer operator for running a program and programmer comments within the program code) became expendable.

Instead of documentation, Customs has relied on four key managers to supply systemwide information and to fill this information gap. The managers—longtime employees who have extensive knowledge of Customs' operations—directly supervise the day-to-day analysis, design, and programming of ACS. They supply most of the information that programmers, primarily contractors, use in designing initial program models and subsequent modifications. They are the only personnel who deal with issues that cut across more than one functional area and who know ACS' software design. Contract employees who program the system told us they generally rely on these managers to interpret user needs and sketch out program designs.

Although we are not aware that Customs has experienced difficulty due to the lack of systemwide documentation, we have observed problems in this area in other agencies. For example, we reported⁶ in 1981 that incomplete documentation in the automated system supporting the Social Security Administration's Supplemental Security Income program's benefit payments had contributed to uncontrolled systems modifications and \$25 million in erroneous payments. Customs' reliance on a few key individuals to synthesize and retain critical information without historical documentation is not an acceptable federal practice. If these key managers were to leave, Customs' ability to maintain ACS' software quality throughout its expected 10-year life would certainly be more difficult and time-consuming.

Customs' Testing Program Needs Test Plans

Software testing is crucial to delivering software-application systems of high quality. Testing measures how well the program under consideration safeguards assets (including sensitive data) and data integrity, how effectively it meets users' functional requirements; how efficiently it operates; and how well it will retain quality throughout its life. Testing also ensures that programs can function correctly and allows for error identification and correction before an organization's operations are adversely affected. Although Customs has established a testing program for ACS, it does not require formal test planning or a formal reporting of test results or systems certification.

⁶Government-wide Guidelines and Management Assistance Center Needed to Improve ADP Systems Development (GAO/AFMD-81-20, February 20, 1981)

Office of Management and Budget Circular A-130 requires that test results for sensitive systems (those that, like ACS, process and store proprietary data) be fully documented and maintained as part of an agency's records. It requires certification of test results and a program of periodic recertification. In addition, the National Bureau of Standards' guidelines state that software testing should receive a level of management attention commensurate with the system's criticality, complexity, and project structure. The standards strongly recommend formally documented plans, specifications, and results from tests, and problem reports for complex, mission-critical systems such as ACS

Customs recognized the importance of these principles when its Office of Data Systems prepared the August 1983 Quality Assurance Test Plan Standard. The standard describes test (1) process planning, (2) methodology, (3) evaluation criteria, (4) controls, inputs, expected outputs, and detailed procedures, and the functions to be tested. However, none of these has been developed for ACS.

The Chief of Customs' Systems Acceptance Test Section told us that the agency generally does not prepare formal test plans because of limited staff and typically tight deadlines. Section staff may do some ad hoc planning before testing complex program functions; any plans developed are not formalized or retained. He also said that test results are not comprehensively reported, although problems encountered during either testing or subsequent program operation are documented and tracked to ensure resolution. Notes and other informal documentation that testers accumulate during program tests are not retained on any systematic basis. He said that as chief he is directly responsible for approving programs for operation and he does so without a formal certification. Another staff member told us that Customs neither prepares test plans nor documents the test results, except for test problem reports

Conclusions

We identified several weaknesses in ACS' internal controls and development procedures, but no actual fraud, waste, or abuse involving ACS. We found

- individuals with access to ACS functions beyond those necessary to perform their assigned jobs; this not only violates the separation of duties principle, but also allows the opportunity for individuals to perform functions and initiate operations on data to commit fraud, then to cover up or remove evidence of their actions;

-
- inadequate documentation of the operational interrelationships among ACS' 15 modules; this risks delay and the introduction of errors when maintaining or modifying ACS, especially if any of the four key managers leave or are otherwise unavailable; and
 - lack of adequate test plans, increasing the risk that the ACS software will contain serious errors.

Any significant frauds, delays, or errors resulting from these weaknesses could compromise Customs' efforts to enforce the nation's trade laws and collect import duties. The possibility that this could occur increases as ACS becomes more complex and becomes an integral part of Customs' operations. Accordingly, we believe these are material control weaknesses that should be reported under provisions of the Federal Managers' Financial Integrity Act (31 U.S.C. 3512 (b) and (c)).

We also believe several steps can be taken to enhance the security and integrity of ACS and provide greater assurance that it operates properly.

Recommendations

We recommend that you

- establish and implement procedures to ensure that employees' functional access to ACS is limited to only those functions to which they need access to perform their assigned duties;
- document how ACS' various modules or functional areas interrelate; and
- develop formal test plans and perform all testing of ACS' application programs under these plans.

In addition, in accordance with the requirements of the Federal Managers' Financial Integrity Act, we recommend that you report the lack of system access controls, documentation, and test plans as material control weaknesses until appropriate controls are in place.

Agency Comments and Our Evaluation

Customs agrees that ACS does have weaknesses. However, it disagrees with certain elements of our findings and conclusions. Specifically, Customs said that we did not identify any actual cases of fraud, waste, or abuse involving ACS. In addition, Customs believes our report implies that ACS employs a lax security system. Notwithstanding these disagreements, the agency is planning corrective actions consistent with our recommendations.

Our report identified weaknesses in ACS' internal controls and development procedures that, unless corrected, will increase the risk that actual cases of fraud, waste, or abuse could occur. These weaknesses are generally those that have led to actual cases in other major systems. Our purpose in reporting these weaknesses is to help Customs avert fraud, waste, or abuse in the future. That no cases have yet been discovered in ACS should provide little solace that none could occur or that none are actually occurring. Cases have existed in other systems for several years before being detected.

Our report makes recommendations that we believe will help reduce ACS' exposure to these risks. Customs believes our report implies that ACS' security is lax; however, our draft report was clear and explicit on this control weakness. We stated that one essential element of system security—password control—is adequate, but another, equally important element—functional access control—is not. Good password control by itself provides a certain level of security, but, as Customs recognizes, both are necessary.

Customs' Commissioner states that he

- personally directed ACS' development and decided that its successful implementation would require streamlined rather than traditional approaches to system development, implementation, and documentation; and
- believed that traditional approaches to documentation were unnecessarily cumbersome, bureaucratic, and time-consuming.

We support successful and timely development of automated systems. The issue of traditional versus nontraditional approaches is separate from the need to document how ACS' various modules or functional areas interrelate. We distinguish between an industry-recognized need to document versus no documentation at all (i.e., only relying upon the memories of key employees). How that documentation is done is not the issue. The Commissioner's comments acknowledged the need to document, but not until " . . . after the ACS system stabilizes and matures. " In our opinion, however, the longer Customs waits to document, the greater the probability the documentation will be incomplete and prone to error.

Based on Customs' comments, we have made technical corrections to the report where appropriate. Customs' comments and our detailed evaluation of them are contained in the appendix.

We are sending copies of this report to the Secretary of the Treasury, the Director, Office of Management and Budget; and interested congressional committees and subcommittees; and will make copies available to others upon request.

Sincerely yours,

A handwritten signature in cursive script that reads "Warren G. Reed". The signature is written in black ink and is positioned below the closing "Sincerely yours,".

Warren G. Reed
Director

Comments From the U.S. Customs Service

Note GAO comments supplementing those in the report text appear at the end of this appendix



THE COMMISSIONER OF CUSTOMS

November 25, 1986

WASHINGTON, D.C.

CO:A:U DFS

Dear Mr. Anderson:

We have reviewed the draft report entitled SYSTEM INTEGRITY: Customs' Automated Commercial System Has Weaknesses and concluded that while some of your observations are accurate and indeed the subject system does have weaknesses, your draft report lacks credibility inasmuch as it contains some inaccurate and unsubstantiated findings, conclusions, and recommendations. I am particularly concerned that your draft report implies that Customs Automated Commercial System (ACS) employs a lax security system and yet acknowledges that you did not identify "actual fraud, waste, or abuse involving ACS." In addition, I am surprised that you have chosen to highlight the lack of ACS documentation without providing evidence that failure to document has contributed to implementation delays and system shortcomings. With the amount of time and effort expended by GAO, and the amount of time Customs employees spent assisting your auditors, the findings seem minor and not consistent with such a negative title.

Before documenting our response to the individual findings, conclusions and recommendations in your draft report, I want to emphasize that I have personally directed the development of ACS. It was early in our ACS development effort that I made the conscious decision that successful implementation of ACS would require streamlined approaches rather than traditional approaches to systems development, implementation and documentation which I believe are unnecessarily cumbersome, bureaucratic, and time consuming. Had we utilized traditional approaches in developing ACS, I am fearful that we would still be documenting the system. Instead, Customs is working with a system that allows it to maintain currency in commercial import processing, fulfill numerous legal and regulatory obligations, and avoid the necessity for requesting large staffing increases.

GAO FINDINGS

Customs has not:

- o established adequate controls to prevent unwarranted access to ACS;
- o documented clearly enough how ACS operates so that modifications can be made with minimal time and effort without introducing errors; and
- o established a reliable testing program to ensure that software is produced that will meet user needs while maintaining system security.

CUSTOMS RESPONSE TO GAO FINDINGS

See comment 1

GAO has failed to recognize that adequate security controls do exist for ACS. Field terminals are usually in secure locations. Users must know sign-on procedures, have a valid I.D., know their password, and can only execute specific functions assigned by a security coordinator. While Customs could accept a finding indicating that administration of functional access needs improvement, it cannot accept a finding implying that ACS security controls are incapable of preventing unwarranted access.

See comment 2

As indicated in the second paragraph of this letter, ACS was and continues to be developed using streamlined approaches. While acknowledging that ACS documentation is minimal, we disagree with the finding that clear documentation on how ACS operates would enable Customs to make modifications with minimal time and effort without introducing errors. As ACS continues to grow in complexity, Customs believes that voluminous documentation would delay rather than accelerate implementation of new ACS features designed to accommodate user and legislative requirements. Because ACS is a rapidly changing system, we believe extensive documentation would become obsolete almost when written. Customs reliance on limited resources for providing quick and accurate system solutions to large operational concerns has permitted implementation of timely and reliable ACS modifications.

See comment 3

A finding that Customs has not "established a reliable testing program to ensure that software is produced that will meet user needs while maintaining system security" is neither supported by Customs experience nor findings in your draft report. Based on the results of three years of ACS operations and the lack of contrary evidence in the draft report, we believe that we have a reliable testing program which meets user needs and ensures maintenance of system security. If this GAO finding stated that Customs' ACS testing program fails to comply with National Bureau of Standards guidelines, Customs could accept it.

GAO CONCLUSIONS

We found:

- o individuals with access to ACS functions beyond those necessary to perform their assigned jobs; this not only violates the separation of duties principle, but allows the opportunity for individuals to perform functions and initiate operations on data to commit fraud, then to cover up or remove evidence of their actions;
- o inadequate documentation of the interrelationships among ACS' 15 modules; this risks delay and the introduction of errors when maintaining or modifying ACS, especially if any of the four key managers leave or is otherwise unavailable; and
- o lack of adequate test plans, increasing the risk that the ACS software will contain serious errors.

CUSTOMS RESPONSE TO GAO CONCLUSIONS

See comment 1

Customs agrees that there are individuals in the Customs Service who have access to ACS functions beyond those necessary to perform their assigned jobs. This problem is not one of system design but rather one of security administration. The ACS system allows us to limit specific individuals to specific functions. The ACS security system is designed to maximize management flexibility in the granting of functional access. It is possible to authorize an individual to enter data corresponding to a particular record and prohibit that same individual from changing the record.

See comment 2

While acknowledging that there is room for improvement in ACS documentation, Customs disagrees with the suggestion that "inadequate documentation of the interrelationships among ACS' 15 modules" will delay implementation and introduce errors when modifying ACS. We disagree with your conclusion because (1) we routinely make numerous changes to ACS to enhance operations and to correct problems without disturbing system integrity or operation; (2) the draft report does not support this conclusion and in fact states - - "we are not aware that Customs has experienced difficulty due to the lack of documentation...;" (3) Customs has a cadre of knowledgeable ACS employees and competent contractor/programmer analysts; and (4) we continue to broaden our base of knowledgeable system managers as ACS matures.

See comment 3

The section of the draft report entitled "CUSTOMS NEEDS A RELIABLE TESTING PROGRAM" suggests that test plans be documented, test results recorded, and all such records be retained on a systematic basis. Customs agrees that formalization of testing is a desirable objective but rejects the aforementioned section heading

See comment 3

because it suggests, without any supporting evidence, that we do not have a reliable testing program for ACS. Furthermore, the draft report fails to include relevant evidence to support the conclusion that lack of adequate test plans increases the risk of introduction of serious ACS software errors. Customs rejects this conclusion. On the basis of our reading of the evidence provided, a conclusion indicating that ACS testing procedures do not comply with National Bureau of Standards guidelines for software testing seems to be appropriate.

GAO RECOMMENDATIONS

- o establish and implement procedures to ensure that employees' functional access to ACS is limited to only those functions they need to perform their assigned duties;
- o document how ACS' various modules or functional areas interrelate; and
- o perform all testing of ACS applications programs under formal test plans.

CUSTOMS RESPONSE TO GAO RECOMMENDATIONS

See comment 1

Because procedures already exist, Customs disagrees that we must establish procedures to ensure that functional access is limited as recommended. We do however agree that effective implementation and improvement of existing procedures is required. To improve the administration of functional access, Customs intends to: issue updated guidelines emphasizing the "separation of duties principle;" initiate periodic field review of assigned functions; and investigate the possibility of transferring responsibility for functional security control to local Customs managers.

See comment 2

As indicated previously in this letter, I believe that documentation is unnecessarily cumbersome, bureaucratic, and time consuming; and I am convinced that the pace at which ACS is being implemented effectively precludes traditional documentation preparation. Because I recognize that documentation will become necessary after the ACS system stabilizes and matures, I have instructed that the Office of Automated Commercial System Operations and the Office of Data Systems examine the availability and feasibility of acquisition of some automated documentation tools to facilitate the documentation process.

See comment 3

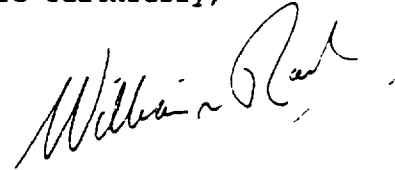
Customs agrees that all testing should be performed under formal test plans. A study is being undertaken to secure automated test aids - - one for playing back transactions and another for tracking execution paths in order to improve the effectiveness and efficiency of the testing process. These improvements will allow us to create formal plans for testing each module and for system integration testing.

Appendix I
Comments From the U.S. Customs Service

ACS was developed to support a field organization that was being buried by an increasing volume of cargo at a time when an increase in personnel was not possible. Recent Customs surveys indicate both a high level of satisfaction with ACS and a heavy reliance on the system. We are handling a dramatically increasing volume of importations without corresponding increases in staff and with greater standardization and data reliability. By any measure, ACS is a resounding success.

As you can tell from the foregoing response, Customs is proud of its success with ACS and believes that your draft report is misleading. Indeed, we are of the opinion that your report is so positive that with minor additions and adjustments, a title such as "SYSTEM IMPLEMENTATION: CUSTOMS' MASSIVE AUTOMATED COMMERCIAL SYSTEM DEVELOPED AND IMPLEMENTED IN RECORD TIME WITHOUT NECESSITY FOR LARGE STAFF, DETAILED DOCUMENTATION, AND FORMALIZED TESTING PLANS" would be more appropriate.

Yours faithfully,



Mr. William J. Anderson
Assistant Comptroller General
General Government Programs
United States General Accounting Office
Washington, D.C. 20548

The following are GAO's comments on the U.S. Customs Service's letter dated November 25, 1986.

GAO Comments

1 Our report identifies two measures—passwords and functional access codes—that Customs has implemented to protect ACS from unauthorized access, fraud, abuse, and extended disruption. We also recognize that a security system has been installed to provide an adequate level of password control. We found that granting functional access codes to individual employees is still not being adequately controlled.

Customs stated that it cannot accept a finding implying that ACS security controls are incapable of preventing unwarranted access, yet it agrees that individuals have access to ACS functions beyond those necessary to perform their assigned jobs. We found no evidence to indicate that the security controls as designed into the system were incapable of controlling functional access to ACS. However, we did find that Customs' administration of authorizing functional access to individual employees was not adequately controlled. We believe that access beyond what is required to perform assigned jobs is unnecessary or unwarranted access that creates an opportunity for employees to initiate and cover up unauthorized transactions on ACS.

Customs disagreed with our recommendation to establish and implement procedures to limit functional access, believing that existing procedures, although adequate, need more effective implementation. To achieve this, Customs stated its intent to (1) issue guidelines on the need for separation of duties; (2) initiate periodic field reviews of assigned functions; and (3) investigate the possibility of transferring responsibility for functional security control to local Customs managers.

At the time of our audit, Customs' procedures for granting functional access were limited solely to the mechanical steps of granting such access. Subsequently, Customs expanded its procedures to recognize that functional access should be restricted to the requirements of the specific job. However, this recognition is included as one of several factors Customs' security administrators are asked to consider when assigning ACS functional authorities to employees. It is not mandatory

We believe security administrators should have required procedures for granting functional access. In the event that Customs does decentralize the responsibility for granting functional access, it becomes even more important for procedures that require the limiting of functional access

Furthermore, regardless of decentralization, these procedures must contain adequate guidance to allow the security administrator(s) to consistently apply the procedure on a case-by-case basis. Without such a procedure, Customs' management risks loss of control over this aspect of ACS' security. Therefore, we believe our recommendation to establish and implement procedures to limit an employee's functional access is appropriate.

Since our finding on page 1 of the draft report implied the need for broader control of access to ACS, we have refined our language in our findings and recommendation to more appropriately focus on unwarranted employee access to ACS functions.

2. Our report identifies documentation as the key element to system and program maintenance, stating that documentation increases the ease and accuracy of maintenance. We point out that Customs has not documented the interrelationships among ACS' 15 distinct modules or functional areas because the agency placed a higher priority on speedy implementation of ACS. Instead of documenting the interrelationships, Customs has relied on the memories of four key managers to provide the information that programmers, primarily contractors, need in designing new programs and modifying old ones.

Customs does not agree that such documentation would enable it to make modifications with minimal time and effort and would minimize the introduction of errors. Customs asserts that documentation would be voluminous and would delay rather than accelerate implementation of new features in ACS' rapidly changing system. More specifically, Customs believes it has demonstrated that it can successfully modify ACS without disturbing system integrity or operation. As evidence, the agency points to the fact that we did not identify any difficulties Customs experienced due to the lack of documentation.

The fact that Customs has chosen a streamlined approach requiring only minimal documentation and that ACS has no known integrity or operational problems does not relieve Customs of the responsibility for documentation that will reduce reliance on the memory of selected individuals. It is the potential for loss of these few, critical individuals—at any time during ACS' life—that concerns us. We did not recommend voluminous documentation, only that Customs document the intermodule relationships, knowledge that presently resides with the key managers. We strongly believe that because, as Customs acknowledges, ACS is growing in complexity, this specific documentation should

be a priority. Both federal guidelines and industry experience underscore the importance of formal documentation for complex, mission-critical systems. Current literature⁷ supports the need for documentation, even in instances when systems are developed using streamlined techniques.

While we did not attempt to determine if the lack of documentation caused delays or introduced errors in modifying and maintaining ACS software, other agencies have encountered such difficulties. In our opinion, the risk that Customs will experience such problems will become high as ACS becomes more developed and complex and as the key people move on to other jobs or retire.

Customs agrees that the documentation for ACS is minimal and that there is room for improvement. The agency plans to examine the availability and feasibility of acquiring some automated tools to facilitate the documentation process after ACS stabilizes and matures. We believe that Customs should proceed now to document the interrelationships of the ACS modules because it could be several years before ACS stabilizes or matures.

3. Our report questions the reliability of Customs' test program for ACS because it does not require formal test planning, formal reporting of test results, or system certification.

Based on the results of 3 years of ACS operations and the lack of contrary evidence in our draft report, Customs believes it has "a reliable testing program which meets user needs and ensures maintenance of system security."⁸

We believe that Customs' use of a streamlined approach to systems development, which relies on rapid system changes, increases the need for more formalized testing, test results reporting, or system certification. Using test plans that offer consistent test procedures and data between existing and new (or changed) parts of a system simply reduces

⁷Various aspects of the need for and importance of documentation for systems developed under streamlined approaches are discussed in "Iterative Development," Datamation, February 15, 1985, p 98, "Developing High Quality Systems Faster," EDP Analysis, June 1986, p 8, "Developing Systems for Prototyping," EDP Analyzer, September 1981, p 14; "Rapid Prototyping," Datamation, August 15, 1984, p 98, and Boar, Bernard H Application Prototyping: A Requirements Definition Strategy for the 80's, John Wiley & Sons, New York, 1984, pp. 77-78 and 94

⁸Customs' response incorrectly quoted our finding. We said " ensures maintenance of system integrity." (Emphasis added.)

the risk of introducing serious errors into the software. We believe that eliminating this risk will reduce Customs' chance of introducing serious errors into ACS' software.

We believe, and Customs agrees, that all testing should be performed under formal test plans. Customs stated that it is studying automated test aids so it can create formal plans for testing of system integration.

Since we recognize that Customs does have a testing program, we have modified the caption on page 6 and our recommendation to address only the need for test plans.

GAO FINDINGS

Customs has not:

- o established adequate controls to prevent unwarranted access to ACS;
- o documented clearly enough how ACS operates so that modifications can be made with minimal time and effort without introducing errors; and
- o established a reliable testing program to ensure that software is produced that will meet user needs while maintaining system security.

CUSTOMS RESPONSE TO GAO FINDINGS

See comment 1

GAO has failed to recognize that adequate security controls do exist for ACS. Field terminals are usually in secure locations. Users must know sign-on procedures, have a valid I.D., know their password, and can only execute specific functions assigned by a security coordinator. While Customs could accept a finding indicating that administration of functional access needs improvement, it cannot accept a finding implying that ACS security controls are incapable of preventing unwarranted access.

See comment 2

As indicated in the second paragraph of this letter, ACS was and continues to be developed using streamlined approaches. While acknowledging that ACS documentation is minimal, we disagree with the finding that clear documentation on how ACS operates would enable Customs to make modifications with minimal time and effort without introducing errors. As ACS continues to grow in complexity, Customs believes that voluminous documentation would delay rather than accelerate implementation of new ACS features designed to accommodate user and legislative requirements. Because ACS is a rapidly changing system, we believe extensive documentation would become obsolete almost when written. Customs reliance on limited resources for providing quick and accurate system solutions to large operational concerns has permitted implementation of timely and reliable ACS modifications.

See comment 3

A finding that Customs has not "established a reliable testing program to ensure that software is produced that will meet user needs while maintaining system security" is neither supported by Customs experience nor findings in your draft report. Based on the results of three years of ACS operations and the lack of contrary evidence in the draft report, we believe that we have a reliable testing program which meets user needs and ensures maintenance of system security. If this GAO finding stated that Customs' ACS testing program fails to comply with National Bureau of Standards guidelines, Customs could accept it.

GAO CONCLUSIONS

We found:

- o individuals with access to ACS functions beyond those necessary to perform their assigned jobs; this not only violates the separation of duties principle, but allows the opportunity for individuals to perform functions and initiate operations on data to commit fraud, then to cover up or remove evidence of their actions;
- o inadequate documentation of the interrelationships among ACS' 15 modules; this risks delay and the introduction of errors when maintaining or modifying ACS, especially if any of the four key managers leave or is otherwise unavailable; and
- o lack of adequate test plans, increasing the risk that the ACS software will contain serious errors.

CUSTOMS RESPONSE TO GAO CONCLUSIONS

See comment 1

Customs agrees that there are individuals in the Customs Service who have access to ACS functions beyond those necessary to perform their assigned jobs. This problem is not one of system design but rather one of security administration. The ACS system allows us to limit specific individuals to specific functions. The ACS security system is designed to maximize management flexibility in the granting of functional access. It is possible to authorize an individual to enter data corresponding to a particular record and prohibit that same individual from changing the record.

See comment 2

While acknowledging that there is room for improvement in ACS documentation, Customs disagrees with the suggestion that "inadequate documentation of the interrelationships among ACS' 15 modules" will delay implementation and introduce errors when modifying ACS. We disagree with your conclusion because (1) we routinely make numerous changes to ACS to enhance operations and to correct problems without disturbing system integrity or operation; (2) the draft report does not support this conclusion and in fact states - - "we are not aware that Customs has experienced difficulty due to the lack of documentation...;" (3) Customs has a cadre of knowledgeable ACS employees and competent contractor/programmer analysts; and (4) we continue to broaden our base of knowledgeable system managers as ACS matures.

See comment 3

The section of the draft report entitled "CUSTOMS NEEDS A RELIABLE TESTING PROGRAM" suggests that test plans be documented, test results recorded, and all such records be retained on a systematic basis. Customs agrees that formalization of testing is a desirable objective but rejects the aforementioned section heading

See comment 3

because it suggests, without any supporting evidence, that we do not have a reliable testing program for ACS. Furthermore, the draft report fails to include relevant evidence to support the conclusion that lack of adequate test plans increases the risk of introduction of serious ACS software errors. Customs rejects this conclusion. On the basis of our reading of the evidence provided, a conclusion indicating that ACS testing procedures do not comply with National Bureau of Standards guidelines for software testing seems to be appropriate.

GAO RECOMMENDATIONS

- o establish and implement procedures to ensure that employees' functional access to ACS is limited to only those functions they need to perform their assigned duties;
- o document how ACS' various modules or functional areas interrelate; and
- o perform all testing of ACS applications programs under formal test plans.

CUSTOMS RESPONSE TO GAO RECOMMENDATIONS

See comment 1

Because procedures already exist, Customs disagrees that we must establish procedures to ensure that functional access is limited as recommended. We do however agree that effective implementation and improvement of existing procedures is required. To improve the administration of functional access, Customs intends to: issue updated guidelines emphasizing the "separation of duties principle;" initiate periodic field review of assigned functions; and investigate the possibility of transferring responsibility for functional security control to local Customs managers.

See comment 2

As indicated previously in this letter, I believe that documentation is unnecessarily cumbersome, bureaucratic, and time consuming; and I am convinced that the pace at which ACS is being implemented effectively precludes traditional documentation preparation. Because I recognize that documentation will become necessary after the ACS system stabilizes and matures, I have instructed that the Office of Automated Commercial System Operations and the Office of Data Systems examine the availability and feasibility of acquisition of some automated documentation tools to facilitate the documentation process.

See comment 3

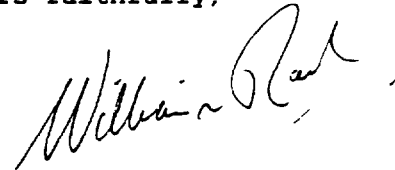
Customs agrees that all testing should be performed under formal test plans. A study is being undertaken to secure automated test aids - - one for playing back transactions and another for tracking execution paths in order to improve the effectiveness and efficiency of the testing process. These improvements will allow us to create formal plans for testing each module and for system integration testing.

Appendix I
Comments From the U.S. Customs Service

ACS was developed to support a field organization that was being buried by an increasing volume of cargo at a time when an increase in personnel was not possible. Recent Customs surveys indicate both a high level of satisfaction with ACS and a heavy reliance on the system. We are handling a dramatically increasing volume of importations without corresponding increases in staff and with greater standardization and data reliability. By any measure, ACS is a resounding success.

As you can tell from the foregoing response, Customs is proud of its success with ACS and believes that your draft report is misleading. Indeed, we are of the opinion that your report is so positive that with minor additions and adjustments, a title such as "SYSTEM IMPLEMENTATION: CUSTOMS' MASSIVE AUTOMATED COMMERCIAL SYSTEM DEVELOPED AND IMPLEMENTED IN RECORD TIME WITHOUT NECESSITY FOR LARGE STAFF, DETAILED DOCUMENTATION, AND FORMALIZED TESTING PLANS" would be more appropriate.

Yours faithfully,



Mr. William J. Anderson
Assistant Comptroller General
General Government Programs
United States General Accounting Office
Washington, D.C. 20548

The following are GAO's comments on the U.S. Customs Service's letter dated November 25, 1986.

GAO Comments

1. Our report identifies two measures—passwords and functional access codes—that Customs has implemented to protect ACS from unauthorized access, fraud, abuse, and extended disruption. We also recognize that a security system has been installed to provide an adequate level of password control. We found that granting functional access codes to individual employees is still not being adequately controlled.

Customs stated that it cannot accept a finding implying that ACS security controls are incapable of preventing unwarranted access, yet it agrees that individuals have access to ACS functions beyond those necessary to perform their assigned jobs. We found no evidence to indicate that the security controls as designed into the system were incapable of controlling functional access to ACS. However, we did find that Customs' administration of authorizing functional access to individual employees was not adequately controlled. We believe that access beyond what is required to perform assigned jobs is unnecessary or unwarranted access that creates an opportunity for employees to initiate and cover up unauthorized transactions on ACS.

Customs disagreed with our recommendation to establish and implement procedures to limit functional access, believing that existing procedures, although adequate, need more effective implementation. To achieve this, Customs stated its intent to (1) issue guidelines on the need for separation of duties; (2) initiate periodic field reviews of assigned functions; and (3) investigate the possibility of transferring responsibility for functional security control to local Customs managers.

At the time of our audit, Customs' procedures for granting functional access were limited solely to the mechanical steps of granting such access. Subsequently, Customs expanded its procedures to recognize that functional access should be restricted to the requirements of the specific job. However, this recognition is included as one of several factors Customs' security administrators are asked to consider when assigning ACS functional authorities to employees. It is not mandatory

We believe security administrators should have required procedures for granting functional access. In the event that Customs does decentralize the responsibility for granting functional access, it becomes even more important for procedures that require the limiting of functional access

Furthermore, regardless of decentralization, these procedures must contain adequate guidance to allow the security administrator(s) to consistently apply the procedure on a case-by-case basis. Without such a procedure, Customs' management risks loss of control over this aspect of ACS' security. Therefore, we believe our recommendation to establish and implement procedures to limit an employee's functional access is appropriate.

Since our finding on page 1 of the draft report implied the need for broader control of access to ACS, we have refined our language in our findings and recommendation to more appropriately focus on unwarranted employee access to ACS functions.

2. Our report identifies documentation as the key element to system and program maintenance, stating that documentation increases the ease and accuracy of maintenance. We point out that Customs has not documented the interrelationships among ACS' 15 distinct modules or functional areas because the agency placed a higher priority on speedy implementation of ACS. Instead of documenting the interrelationships, Customs has relied on the memories of four key managers to provide the information that programmers, primarily contractors, need in designing new programs and modifying old ones.

Customs does not agree that such documentation would enable it to make modifications with minimal time and effort and would minimize the introduction of errors. Customs asserts that documentation would be voluminous and would delay rather than accelerate implementation of new features in ACS' rapidly changing system. More specifically, Customs believes it has demonstrated that it can successfully modify ACS without disturbing system integrity or operation. As evidence, the agency points to the fact that we did not identify any difficulties Customs experienced due to the lack of documentation.

The fact that Customs has chosen a streamlined approach requiring only minimal documentation and that ACS has no known integrity or operational problems does not relieve Customs of the responsibility for documentation that will reduce reliance on the memory of selected individuals. It is the potential for loss of these few, critical individuals—at any time during ACS' life—that concerns us. We did not recommend voluminous documentation, only that Customs document the intermodule relationships, knowledge that presently resides with the key managers. We strongly believe that because, as Customs acknowledges, ACS is growing in complexity, this specific documentation should

be a priority. Both federal guidelines and industry experience underscore the importance of formal documentation for complex, mission-critical systems. Current literature⁷ supports the need for documentation, even in instances when systems are developed using streamlined techniques.

While we did not attempt to determine if the lack of documentation caused delays or introduced errors in modifying and maintaining ACS software, other agencies have encountered such difficulties. In our opinion, the risk that Customs will experience such problems will become high as ACS becomes more developed and complex and as the key people move on to other jobs or retire.

Customs agrees that the documentation for ACS is minimal and that there is room for improvement. The agency plans to examine the availability and feasibility of acquiring some automated tools to facilitate the documentation process after ACS stabilizes and matures. We believe that Customs should proceed now to document the interrelationships of the ACS modules because it could be several years before ACS stabilizes or matures.

3. Our report questions the reliability of Customs' test program for ACS because it does not require formal test planning, formal reporting of test results, or system certification.

Based on the results of 3 years of ACS operations and the lack of contrary evidence in our draft report, Customs believes it has "a reliable testing program which meets user needs and ensures maintenance of system security."⁸

We believe that Customs' use of a streamlined approach to systems development, which relies on rapid system changes, increases the need for more formalized testing, test results reporting, or system certification. Using test plans that offer consistent test procedures and data between existing and new (or changed) parts of a system simply reduces

⁷Various aspects of the need for and importance of documentation for systems developed under streamlined approaches are discussed in: "Iterative Development," Datamation, February 15, 1985, p. 98; "Developing High Quality Systems Faster," EDP Analysis, June 1986, p. 8; "Developing Systems for Prototyping," EDP Analyzer, September 1981, p. 14; "Rapid Prototyping," Datamation, August 15, 1984, p. 98; and Boar, Bernard H. Application Prototyping: A Requirements Definition Strategy for the 80's, John Wiley & Sons, New York, 1984, pp. 77-78 and 94.

⁸Customs' response incorrectly quoted our finding. We said " . . . ensures maintenance of system integrity." (Emphasis added)

the risk of introducing serious errors into the software. We believe that eliminating this risk will reduce Customs' chance of introducing serious errors into ACS' software.

We believe, and Customs agrees, that all testing should be performed under formal test plans. Customs stated that it is studying automated test aids so it can create formal plans for testing of system integration.

Since we recognize that Customs does have a testing program, we have modified the caption on page 6 and our recommendation to address only the need for test plans.

Requests for copies of GAO reports should be sent to:

U.S. General Accounting Office
Post Office Box 6015
Gaithersburg, Maryland 20877

Telephone 202-275-6241

The first five copies of each report are free. Additional copies are \$2.00 each.

There is a 25% discount on orders for 100 or more copies mailed to a single address.

Orders must be prepaid by cash or by check or money order made out to the Superintendent of Documents.

United States
General Accounting Office
Washington, D.C. 20548

Official Business
Penalty for Private Use \$300

Address Correction Requested

First-Class Mail
Postage & Fees Paid
GAO
Permit No G100