United States General Accounting Office

GAO

Report to Congressional Requesters

September 2001

# EDUCATION INFORMATION SECURITY

## Improvements Made But Control Weaknesses Remain

GAO

Accountability * Integrity * Reliability

GAO-01-1067

# Contents

## Letter

## Appendixes

GAO
Accountability ★ Integrity ★ Reliability

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

September 12, 2001

The Honorable Peter Hoekstra
Chairman, Subcommittee on Select Education
Committee on Education and the Workforce
House of Representatives

The Honorable Charlie Norwood
House of Representatives

The Department of Education places significant reliance on its Central Automated Processing System (EDCAPS) to support the department's core financial management information functions, including general ledger and funds management, grant planning and payment processing, and purchasing and contract management. In the past, Education's Inspector General (IG) has reported serious information system control weaknesses in this system. Such reported weaknesses in information system controls increased the risk of unauthorized access or disruption of services and made Education's sensitive grant and loan data vulnerable to inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction, which could have occurred without being detected.

At your request, we assessed the general controls over EDCAPS.[1] On July 24, 2001, we briefed the Chairman on the results of our assessment. The briefing slides are included as appendix I. The purpose of this letter is to provide the published briefing slides to you and to officially transmit our recommendations to the Secretary of Education.

In summary, we found that Education has made progress in correcting security weaknesses identified by Education's IG, and that the department has taken other actions to improve security. However, we identified weaknesses that place critical financial and sensitive grant information at risk of unauthorized access and disclosure, and key operations at risk of disruption. Specifically, Education did not sufficiently protect its network

[1] General controls affect the overall effectiveness and security of computer operations as opposed to being unique to any specific computer application. They include security management, operating procedures, software security features, and physical protection designed to ensure that access to data and programs is appropriately restricted, only authorized changes are made to computer programs, computer security duties are segregated, and backup and recovery plans are adequate to ensure the continuity of essential operations.

from unauthorized users, effectively manage user IDs and passwords, appropriately limit access to authorized users, effectively maintain system software controls, or routinely monitor user access activity. Further, Education was not providing adequate physical security for its computer resources, appropriately segregating all key operational and computer functions, effectively controlling changes to its applications, or fully addressing all aspects of its service continuity needs. A primary reason for the computer security weaknesses was that Education had not yet fully implemented a comprehensive computer security management program. After we completed our fieldwork, Education stated it had corrected some of the weaknesses we identified and had developed a corrective action plan to address the remaining weaknesses.

## Recommendations for Executive Action

We recommend that the Secretary of Education direct the Chief Information Officer and the Chief Financial Officer to ensure that the following actions are completed.

- Correct the information system control weaknesses related to access authority, system software, network security, user ID and password management, access monitoring, physical access, segregation of duties, application program changes, and service continuity.
- Fully implement a comprehensive departmentwide computer security management program. Such a program would include (1) coordination of security management activities; (2) ongoing assessment of risk; (3) comprehensive security awareness training; (4) complete security policies, procedures, and standards; and (5) a program to routinely monitor and evaluate the effectiveness of information system controls.

## Agency Comments

In written comments on a draft of this report, which are reprinted in appendix II, the Deputy Secretary agreed with our recommendations and stated that Education had developed a corrective action plan. He also reported that Education is taking steps to further strengthen and develop a more comprehensive information security program.

As agreed, we are sending copies to members of the House Committee on Education and the Workforce. We are also sending copies to the Secretary of Education and the Director, Office of Management and Budget. This report will also be available on GAO's home page at www.gao.gov. If you have any questions, please contact me at (202) 512-3317 or Dave Irvin, Assistant Director, at (214) 777-5716. We can also be reached at daceyr@gao.gov and irvind@gao.gov. Key contributors to this report are listed in appendix III.

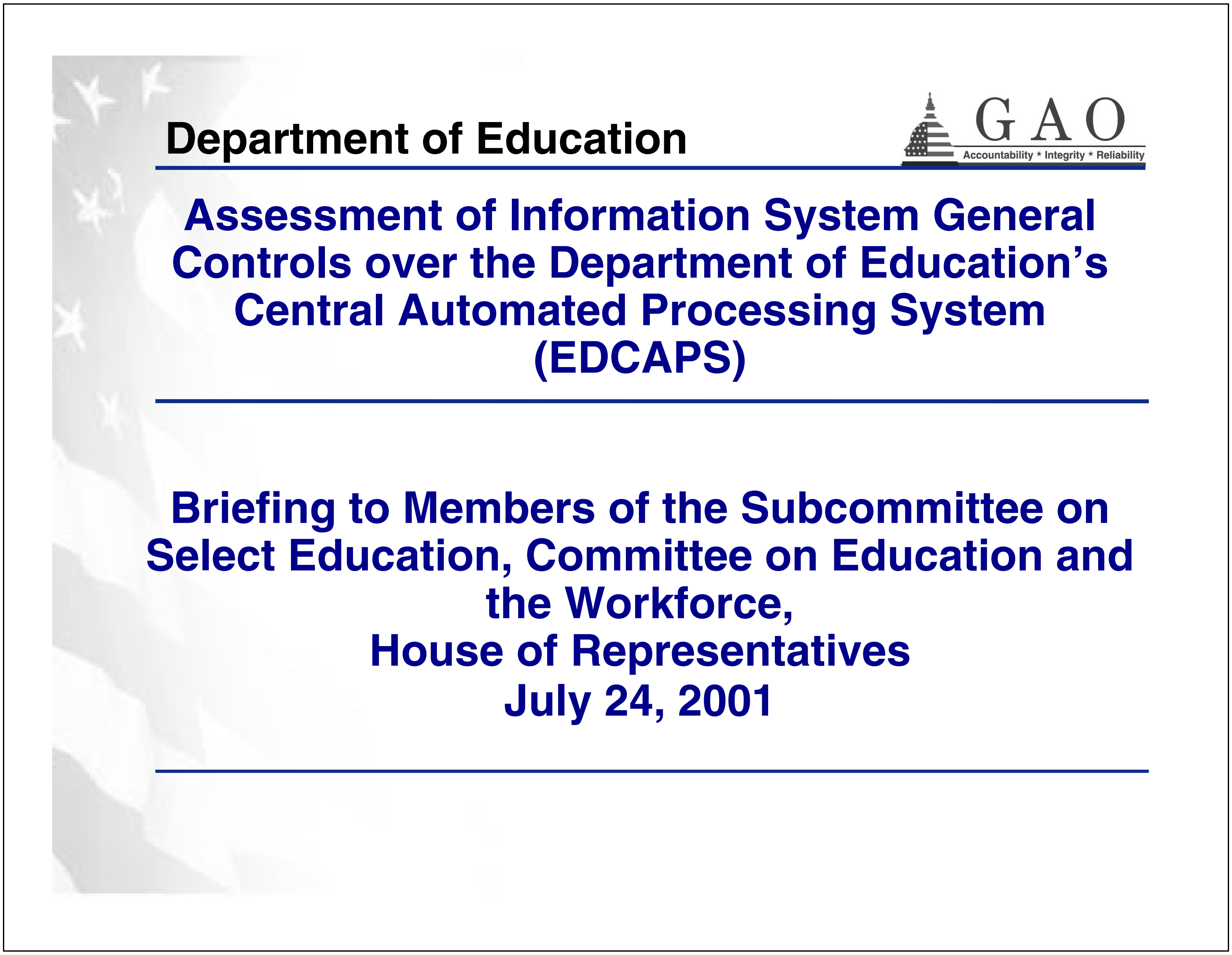
Sincerely yours,

Robert F. Dacey

Robert F. Dacey
Director, Information Security Issues

Appendix I

# GAO's July 24, 2001 Briefing

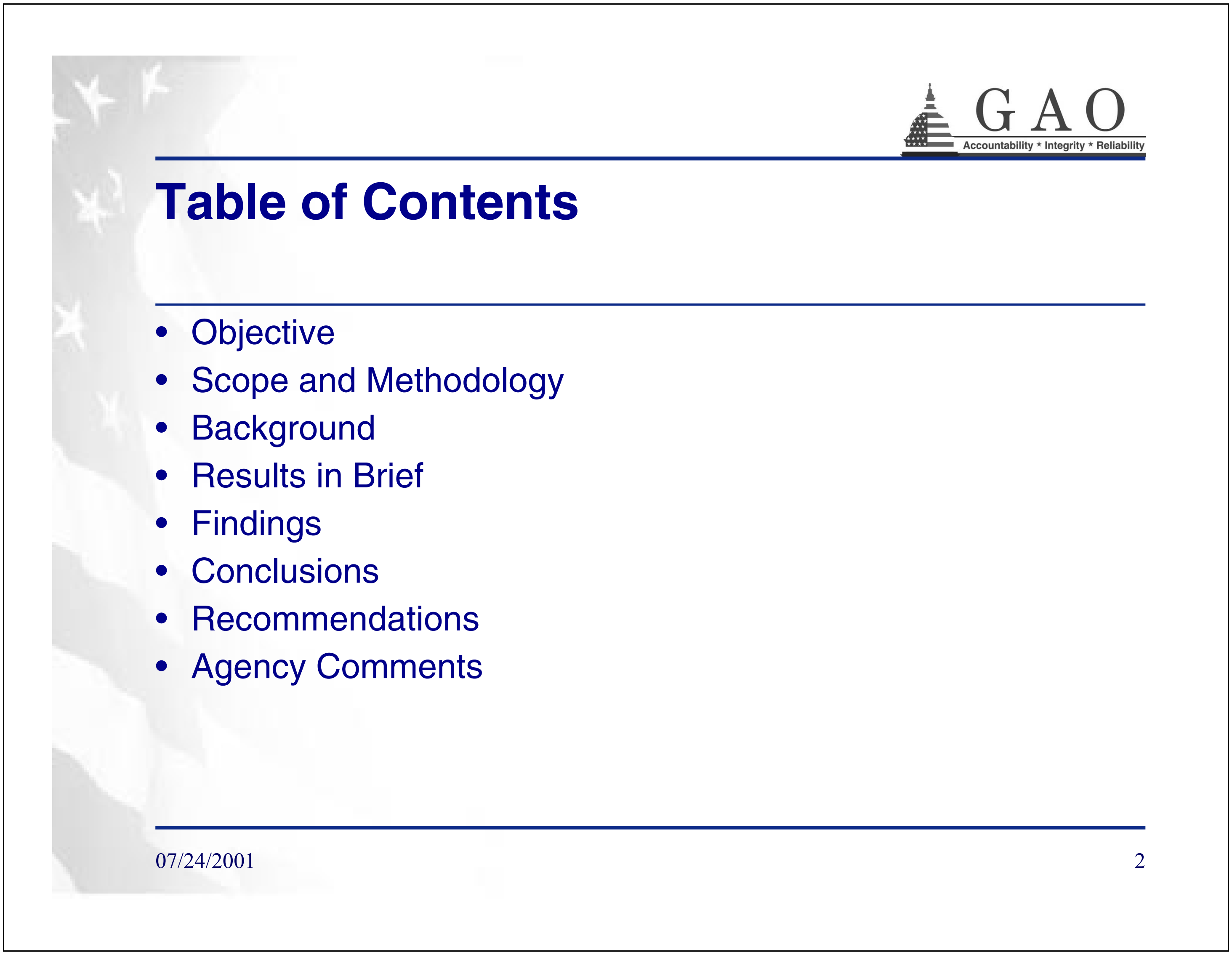


Department of Education

GAO
Accountability * Integrity * Reliability

## Assessment of Information System General Controls over the Department of Education's Central Automated Processing System (EDCAPS)

Briefing to Members of the Subcommittee on Select Education, Committee on Education and the Workforce,
House of Representatives
July 24, 2001

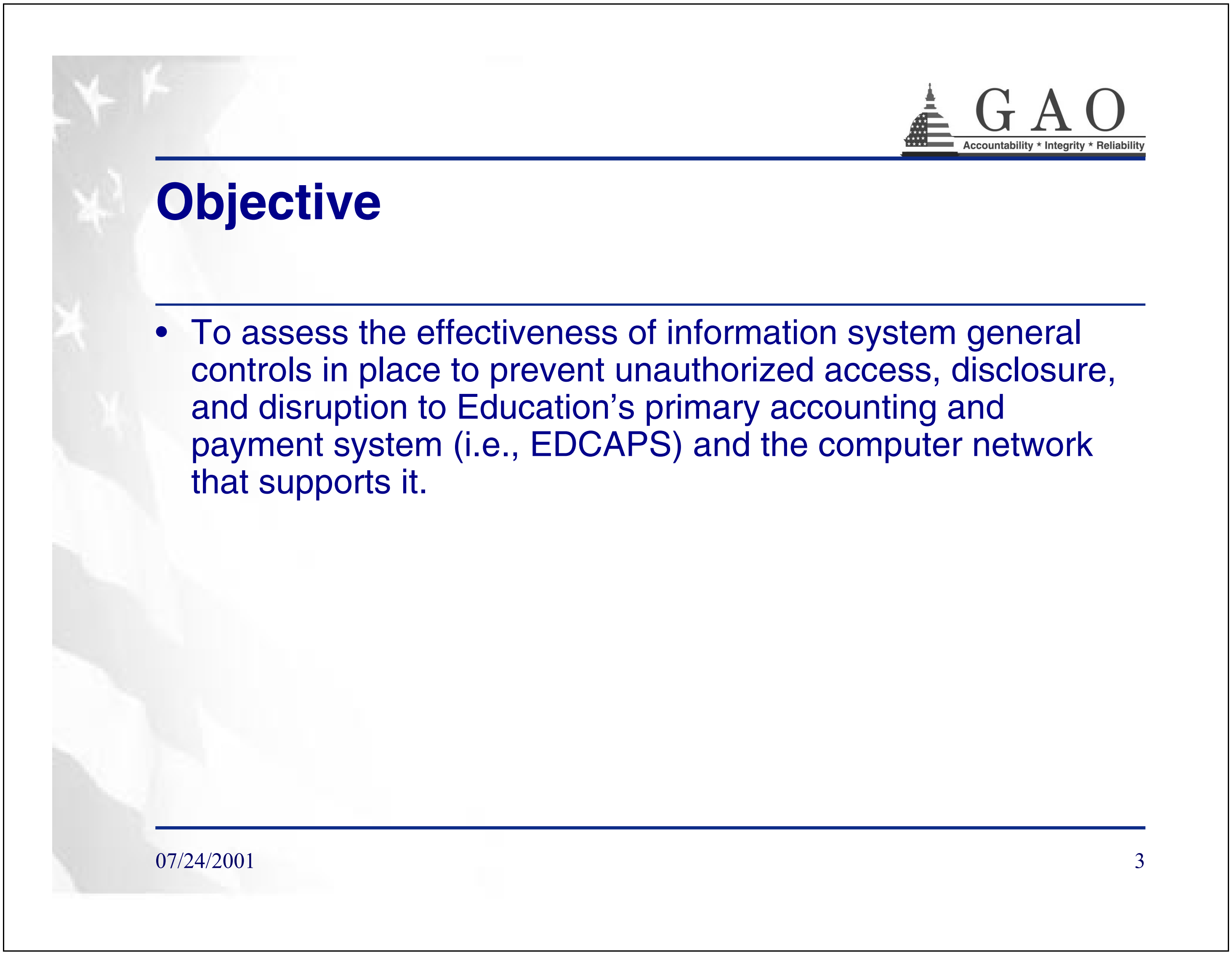


GAO
Accountability * Integrity * Reliability

# Table of Contents

- Objective
- Scope and Methodology
- Background
- Results in Brief
- Findings
- Conclusions
- Recommendations
- Agency Comments

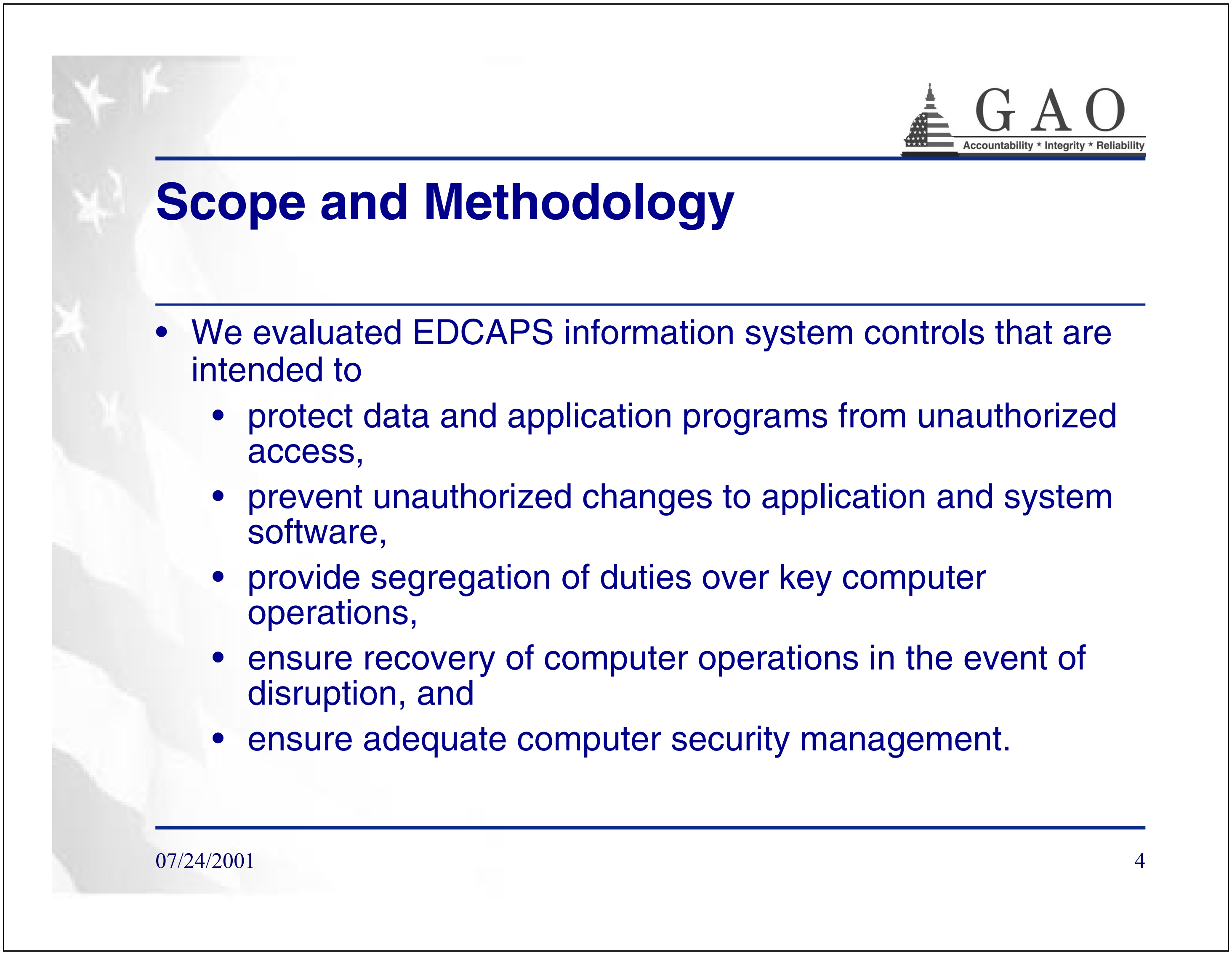
07/24/2001 2



## Objective

- To assess the effectiveness of information system general controls in place to prevent unauthorized access, disclosure, and disruption to Education's primary accounting and payment system (i.e., EDCAPS) and the computer network that supports it.

07/24/2001 3

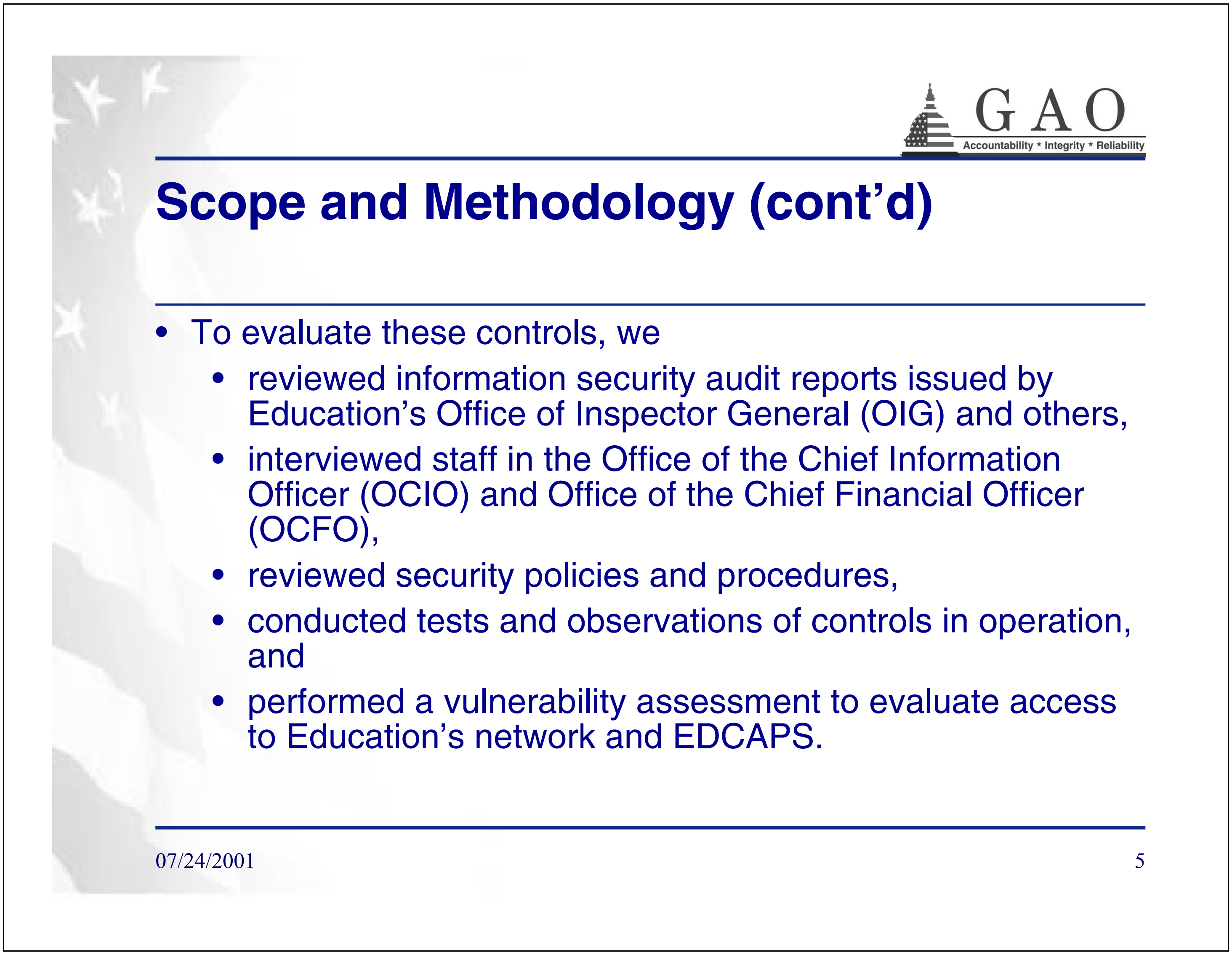


GAO
Accountability * Integrity * Reliability

## Scope and Methodology

- We evaluated EDCAPS information system controls that are intended to
  - protect data and application programs from unauthorized access,
  - prevent unauthorized changes to application and system software,
  - provide segregation of duties over key computer operations,
  - ensure recovery of computer operations in the event of disruption, and
  - ensure adequate computer security management.

07/24/2001 4

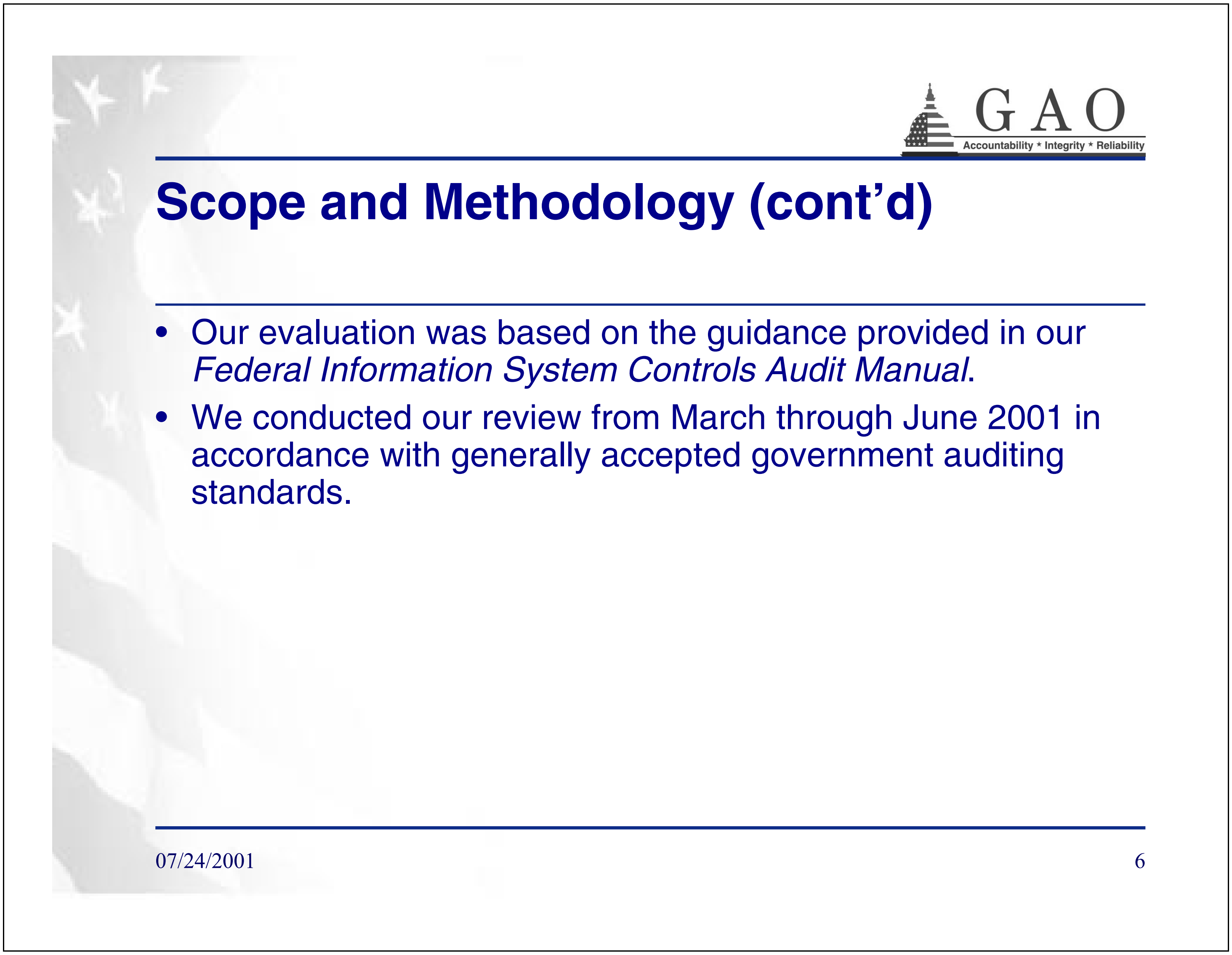


GAO
Accountability * Integrity * Reliability

## Scope and Methodology (cont'd)

- To evaluate these controls, we
  - reviewed information security audit reports issued by Education's Office of Inspector General (OIG) and others,
  - interviewed staff in the Office of the Chief Information Officer (OCIO) and Office of the Chief Financial Officer (OCFO),
  - reviewed security policies and procedures,
  - conducted tests and observations of controls in operation, and
  - performed a vulnerability assessment to evaluate access to Education's network and EDCAPS.

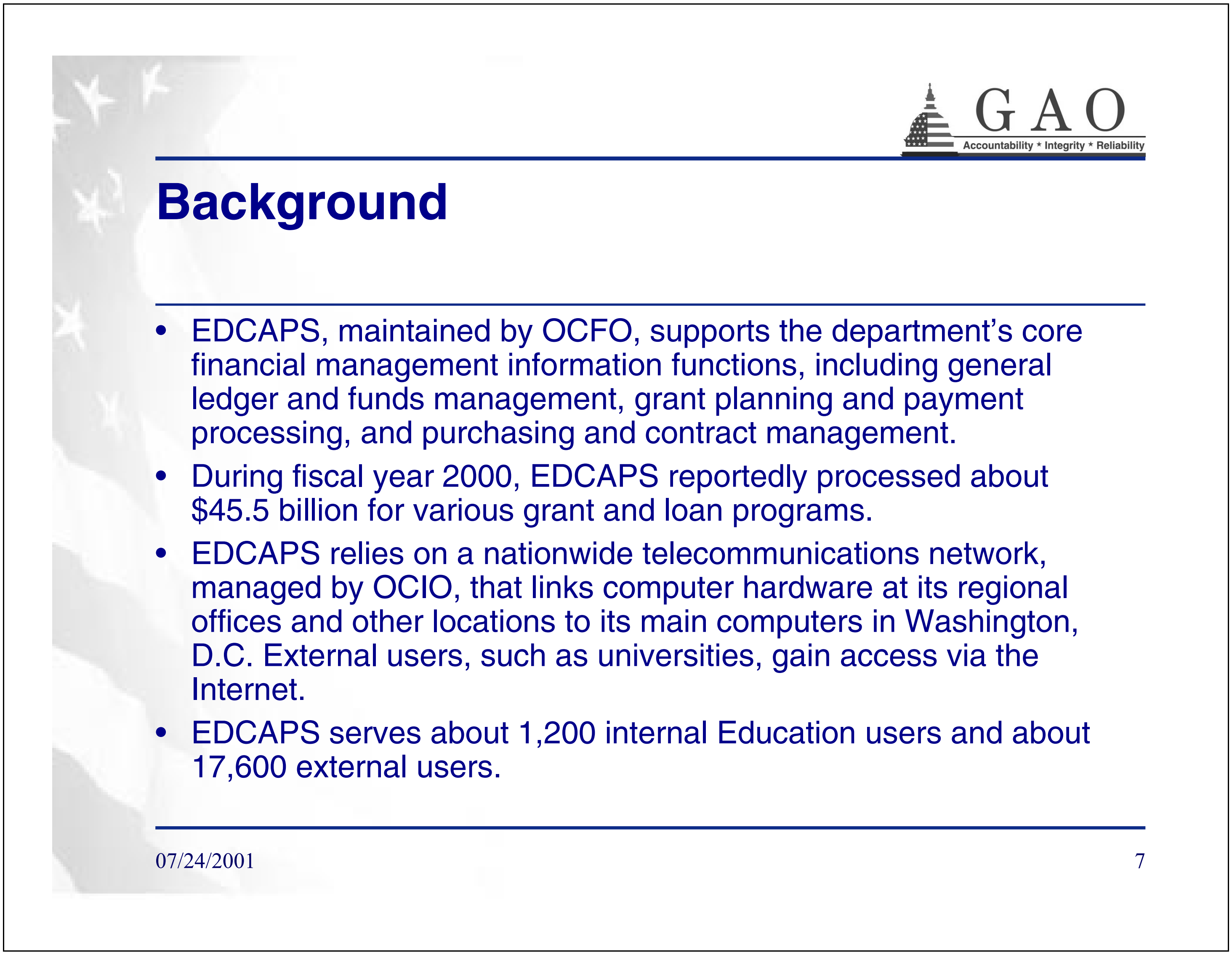
07/24/2001 5



## Scope and Methodology (cont'd)

- Our evaluation was based on the guidance provided in our *Federal Information System Controls Audit Manual*.
- We conducted our review from March through June 2001 in accordance with generally accepted government auditing standards.

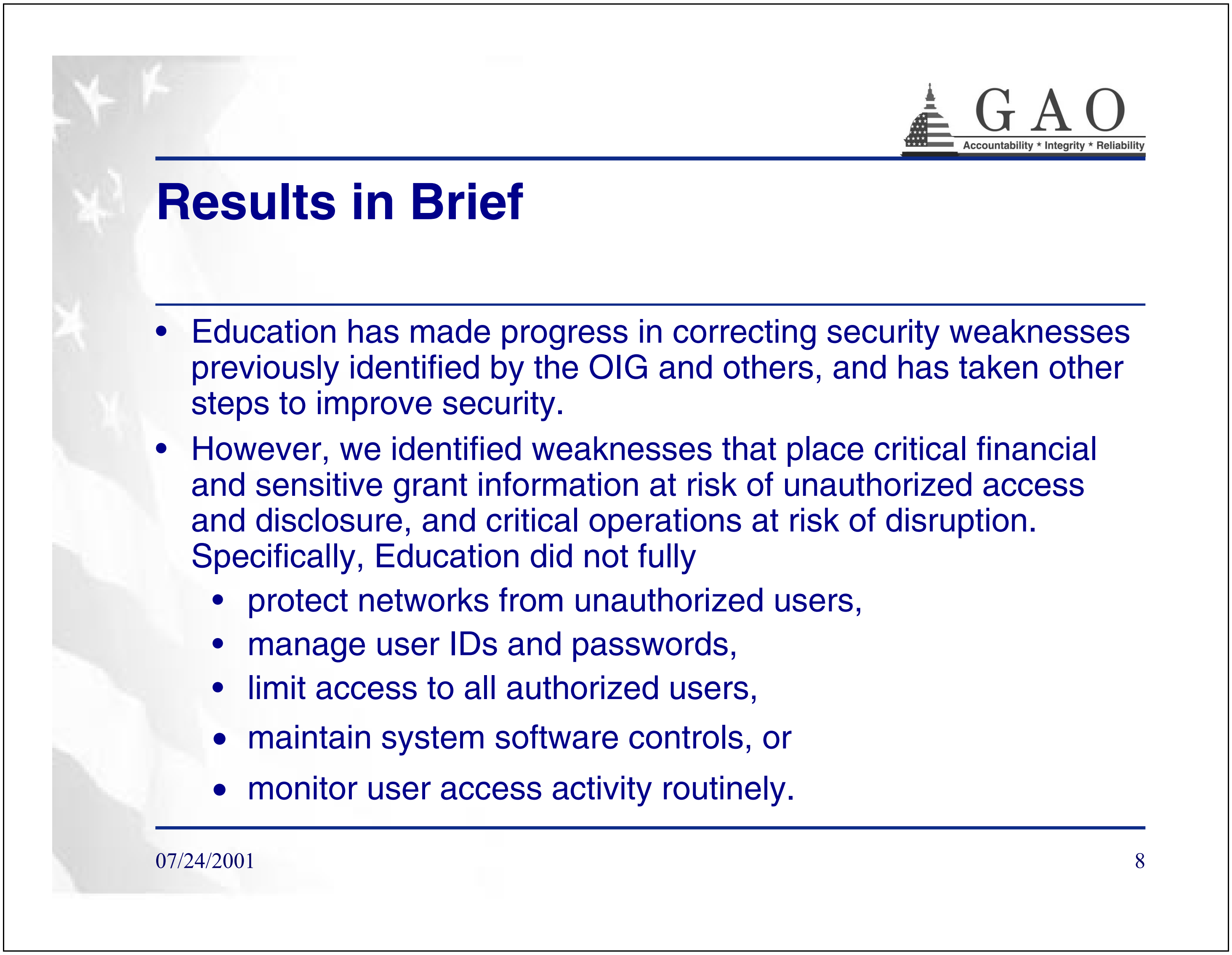
07/24/2001 6



## Background

- EDCAPS, maintained by OCFO, supports the department's core financial management information functions, including general ledger and funds management, grant planning and payment processing, and purchasing and contract management.
- During fiscal year 2000, EDCAPS reportedly processed about $45.5 billion for various grant and loan programs.
- EDCAPS relies on a nationwide telecommunications network, managed by OCIO, that links computer hardware at its regional offices and other locations to its main computers in Washington, D.C. External users, such as universities, gain access via the Internet.
- EDCAPS serves about 1,200 internal Education users and about 17,600 external users.

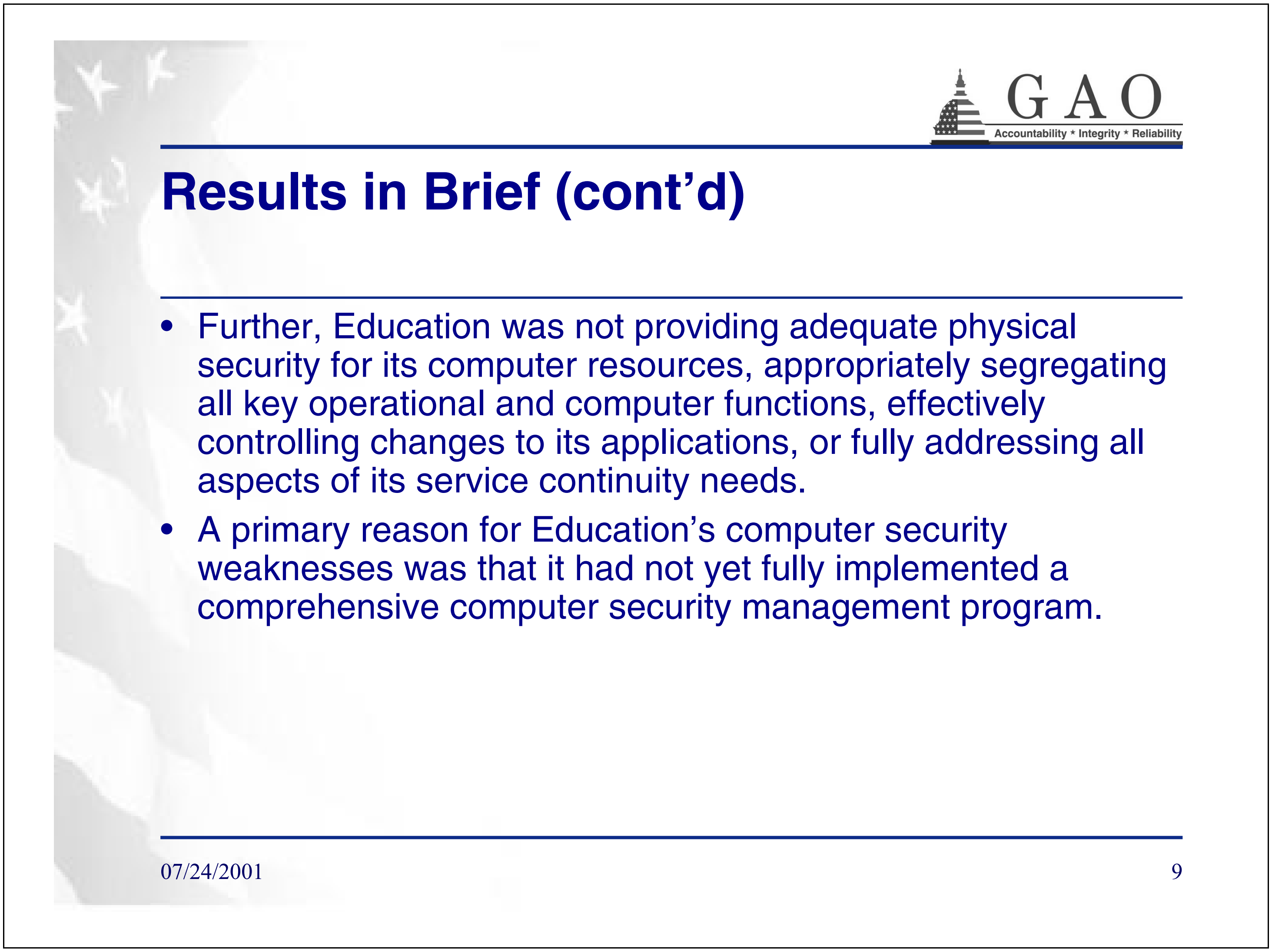
07/24/2001 7



## Results in Brief

- Education has made progress in correcting security weaknesses previously identified by the OIG and others, and has taken other steps to improve security.
- However, we identified weaknesses that place critical financial and sensitive grant information at risk of unauthorized access and disclosure, and critical operations at risk of disruption. Specifically, Education did not fully
  - protect networks from unauthorized users,
  - manage user IDs and passwords,
  - limit access to all authorized users,
  - maintain system software controls, or
  - monitor user access activity routinely.

07/24/2001 8

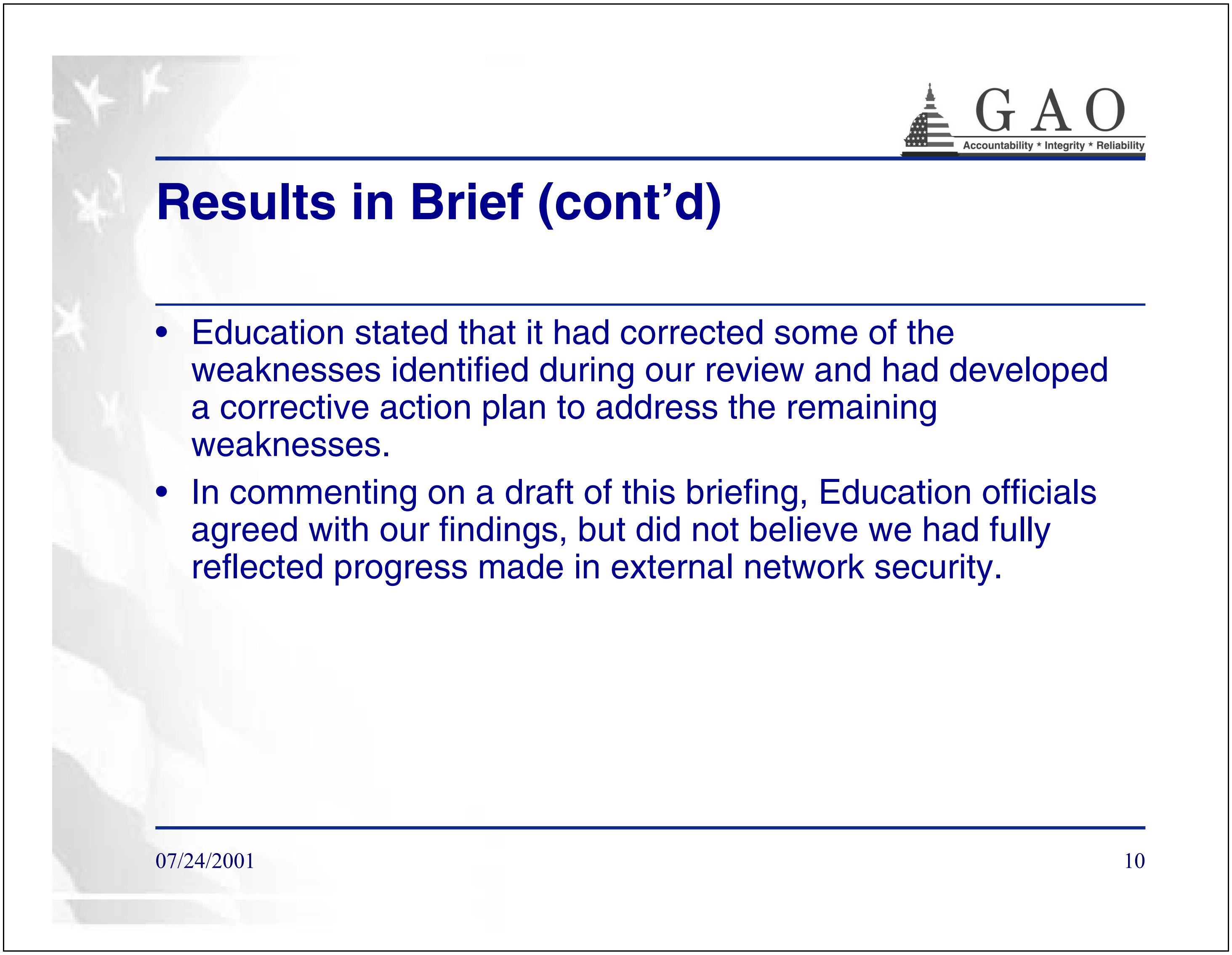


GAO
Accountability * Integrity * Reliability

# Results in Brief (cont’d)

- Further, Education was not providing adequate physical security for its computer resources, appropriately segregating all key operational and computer functions, effectively controlling changes to its applications, or fully addressing all aspects of its service continuity needs.
- A primary reason for Education’s computer security weaknesses was that it had not yet fully implemented a comprehensive computer security management program.

07/24/2001 9

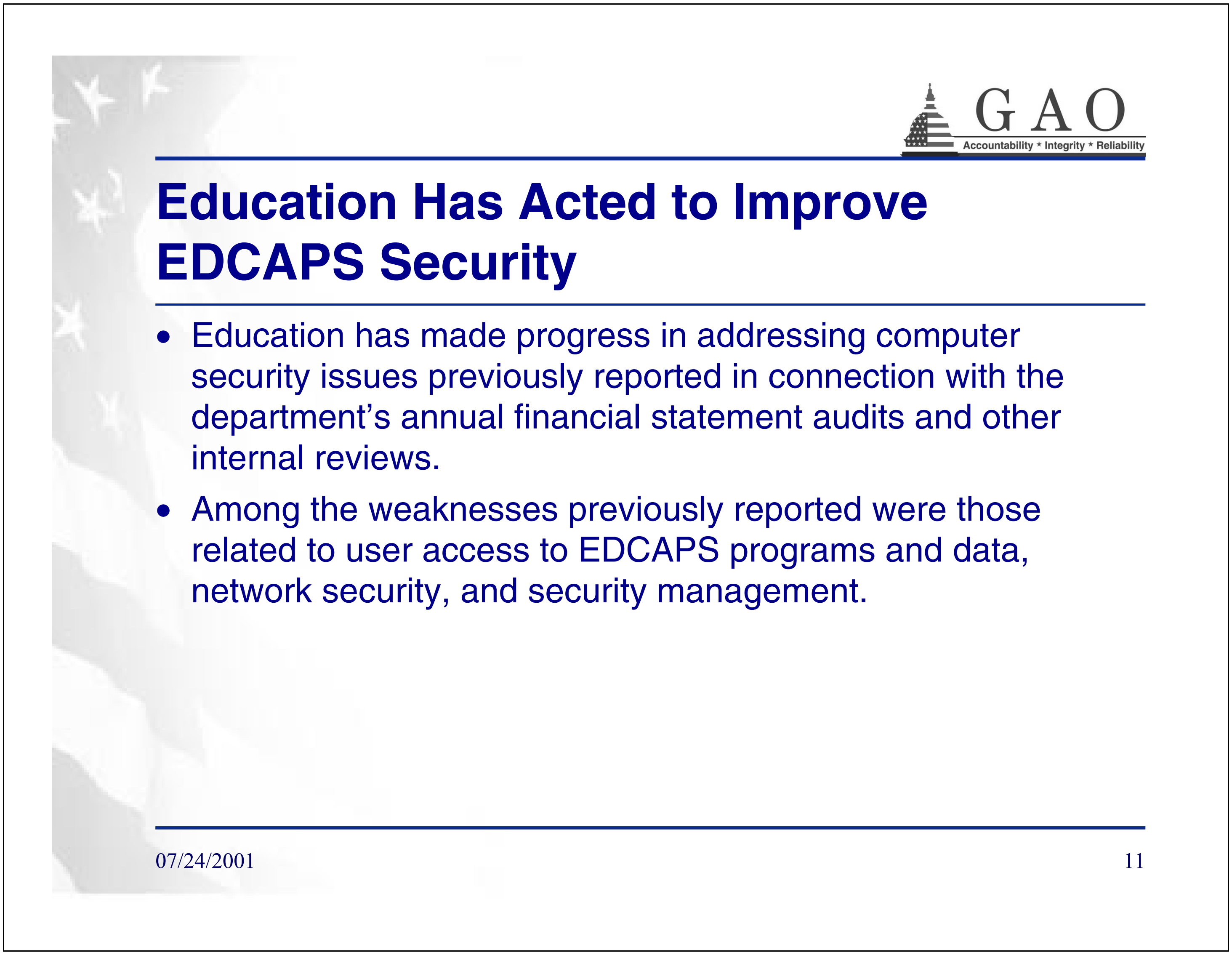


GAO
Accountability * Integrity * Reliability

## Results in Brief (cont'd)

- Education stated that it had corrected some of the weaknesses identified during our review and had developed a corrective action plan to address the remaining weaknesses.
- In commenting on a draft of this briefing, Education officials agreed with our findings, but did not believe we had fully reflected progress made in external network security.

07/24/2001 10

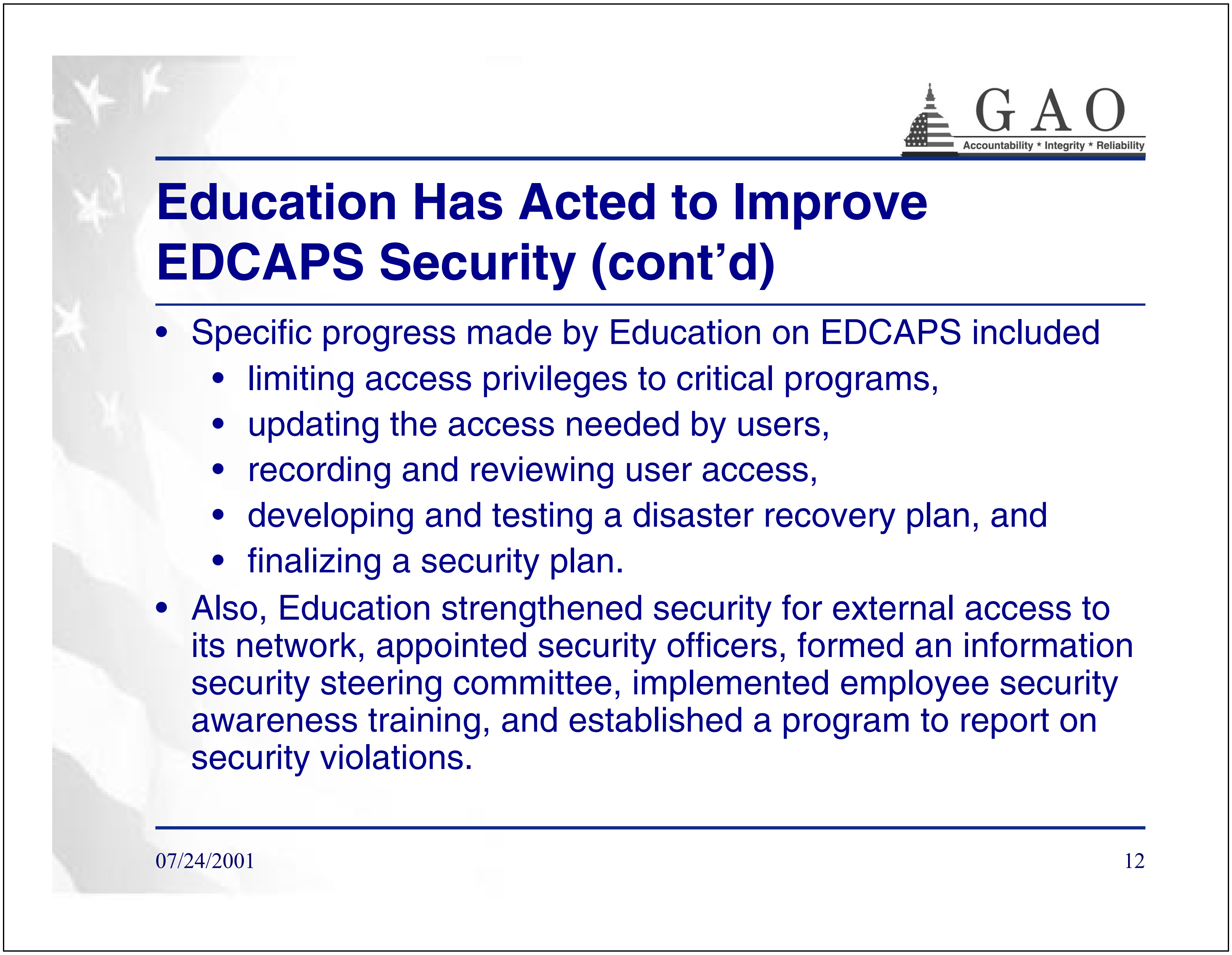


GAO
Accountability * Integrity * Reliability

## Education Has Acted to Improve EDCAPS Security

- Education has made progress in addressing computer security issues previously reported in connection with the department's annual financial statement audits and other internal reviews.
- Among the weaknesses previously reported were those related to user access to EDCAPS programs and data, network security, and security management.

07/24/2001 11

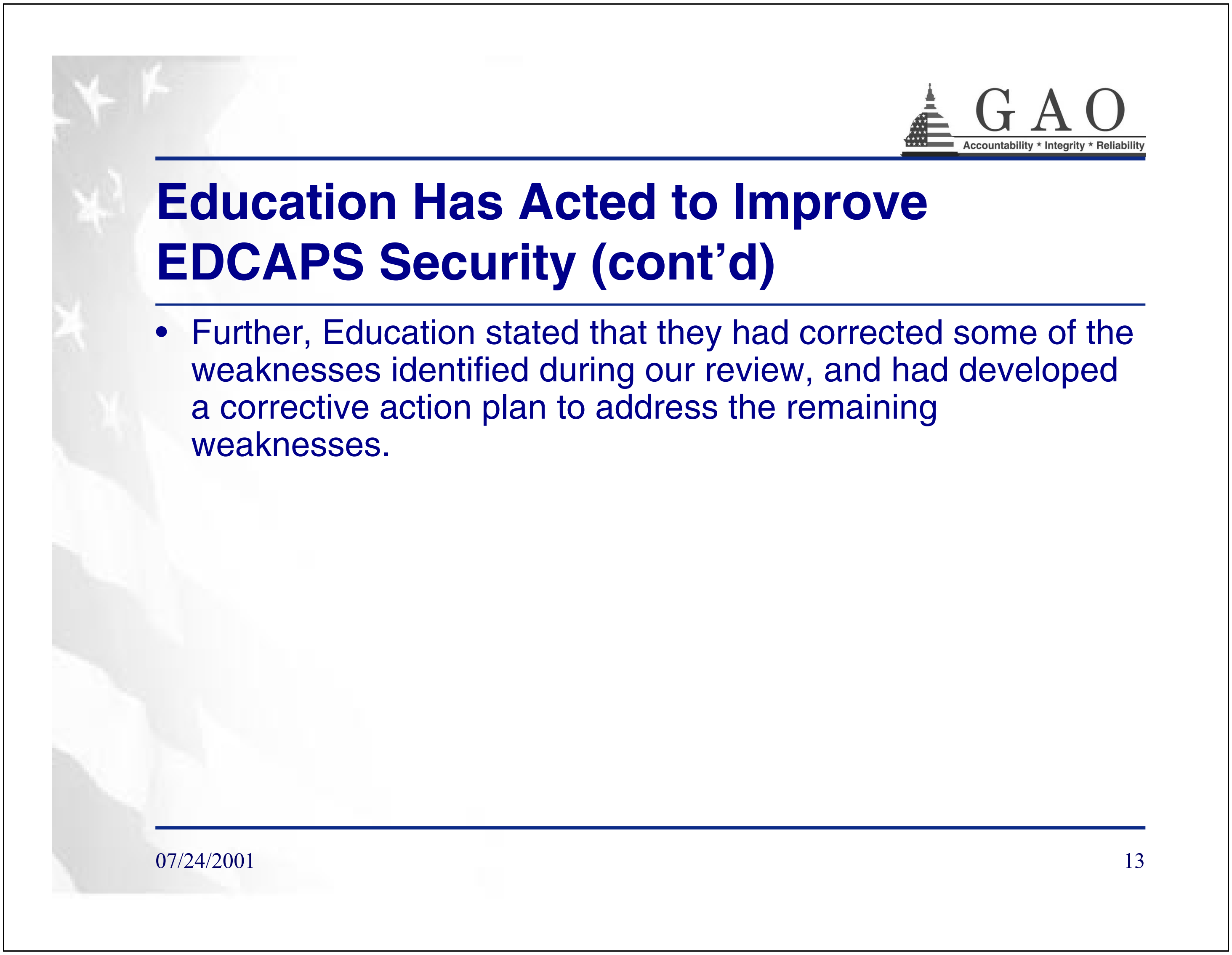


GAO
Accountability * Integrity * Reliability

## Education Has Acted to Improve EDCAPS Security (cont'd)

- Specific progress made by Education on EDCAPS included
  - limiting access privileges to critical programs,
  - updating the access needed by users,
  - recording and reviewing user access,
  - developing and testing a disaster recovery plan, and
  - finalizing a security plan.
- Also, Education strengthened security for external access to its network, appointed security officers, formed an information security steering committee, implemented employee security awareness training, and established a program to report on security violations.

07/24/2001 12

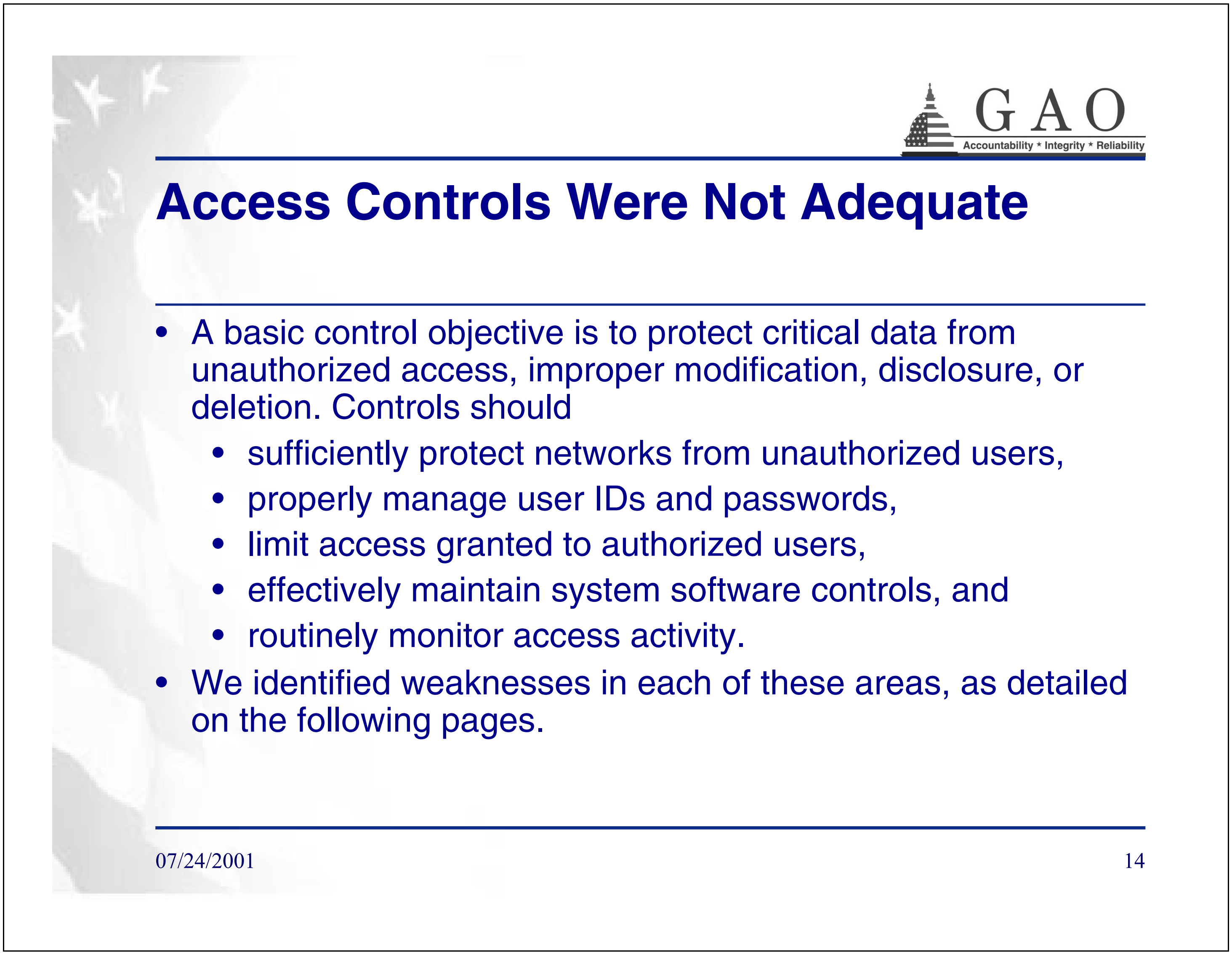


GAO
Accountability * Integrity * Reliability

## Education Has Acted to Improve EDCAPS Security (cont'd)

- Further, Education stated that they had corrected some of the weaknesses identified during our review, and had developed a corrective action plan to address the remaining weaknesses.

07/24/2001 13

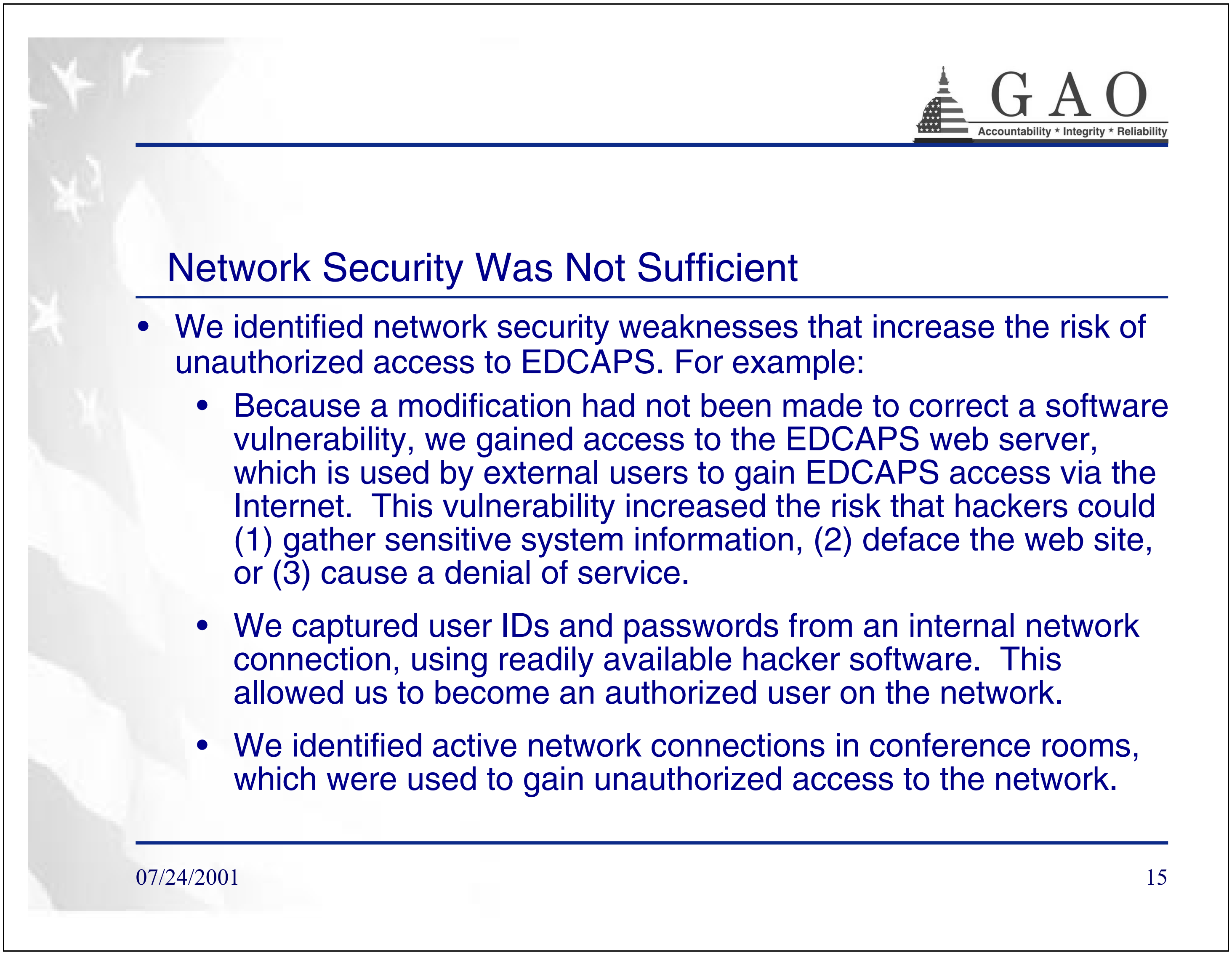


GAO
Accountability * Integrity * Reliability

## Access Controls Were Not Adequate

- A basic control objective is to protect critical data from unauthorized access, improper modification, disclosure, or deletion. Controls should
  - sufficiently protect networks from unauthorized users,
  - properly manage user IDs and passwords,
  - limit access granted to authorized users,
  - effectively maintain system software controls, and
  - routinely monitor access activity.
- We identified weaknesses in each of these areas, as detailed on the following pages.

07/24/2001 14

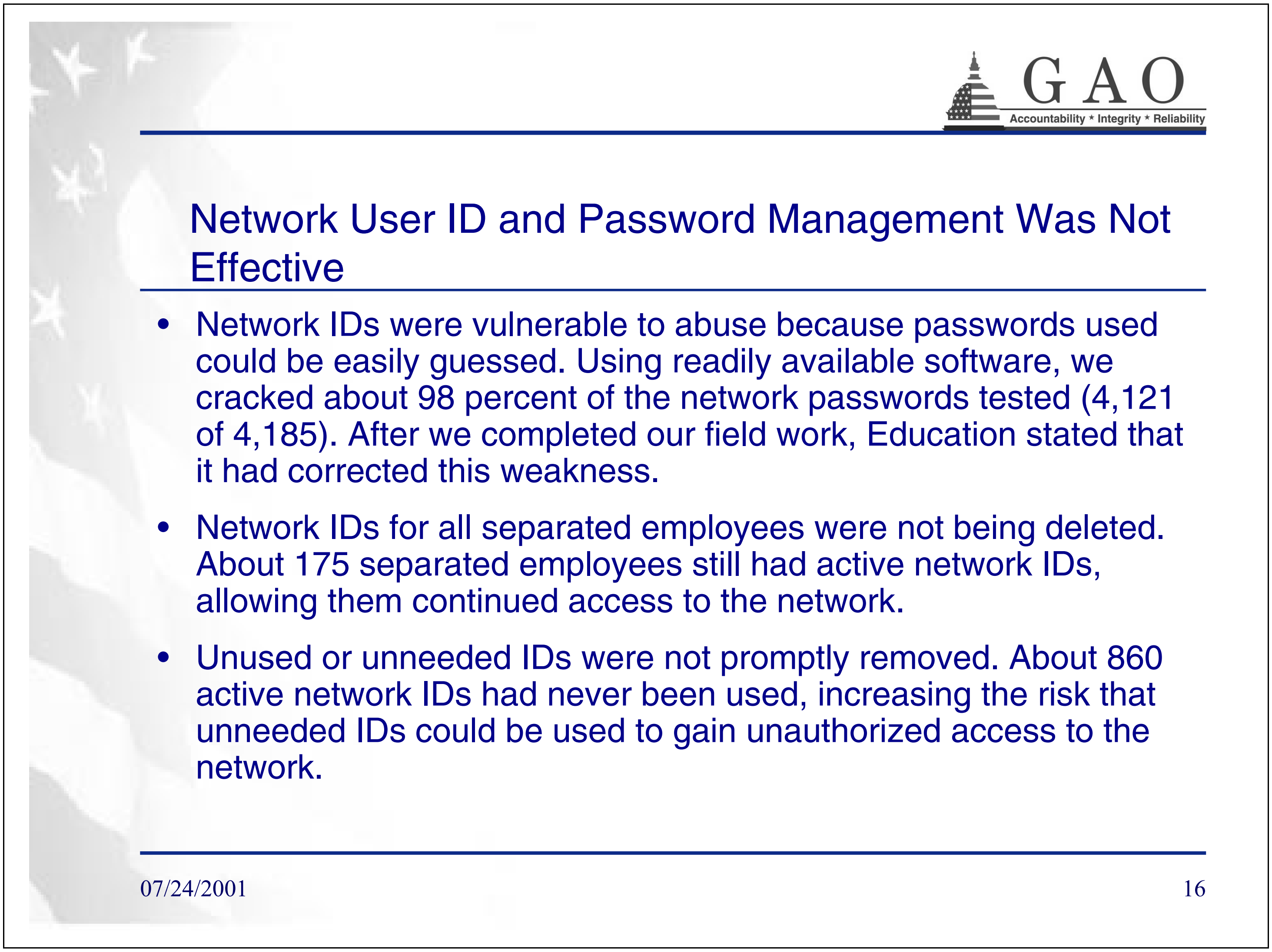


GAO
Accountability * Integrity * Reliability

## Network Security Was Not Sufficient

- We identified network security weaknesses that increase the risk of unauthorized access to EDCAPS. For example:
  - Because a modification had not been made to correct a software vulnerability, we gained access to the EDCAPS web server, which is used by external users to gain EDCAPS access via the Internet. This vulnerability increased the risk that hackers could (1) gather sensitive system information, (2) deface the web site, or (3) cause a denial of service.
  - We captured user IDs and passwords from an internal network connection, using readily available hacker software. This allowed us to become an authorized user on the network.
  - We identified active network connections in conference rooms, which were used to gain unauthorized access to the network.

07/24/2001 15

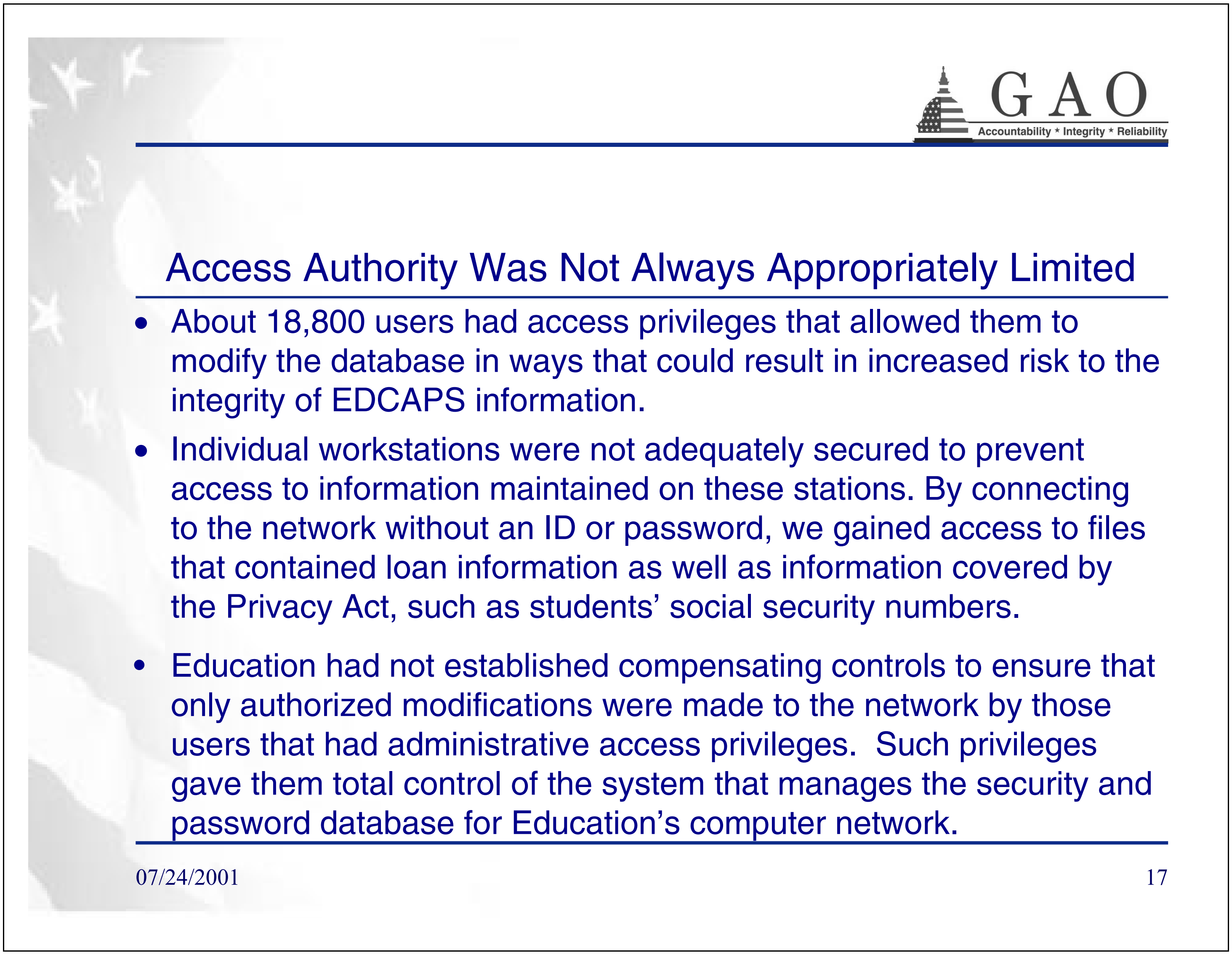


GAO
Accountability * Integrity * Reliability

## Network User ID and Password Management Was Not Effective

- Network IDs were vulnerable to abuse because passwords used could be easily guessed. Using readily available software, we cracked about 98 percent of the network passwords tested (4,121 of 4,185). After we completed our field work, Education stated that it had corrected this weakness.
- Network IDs for all separated employees were not being deleted. About 175 separated employees still had active network IDs, allowing them continued access to the network.
- Unused or unneeded IDs were not promptly removed. About 860 active network IDs had never been used, increasing the risk that unneeded IDs could be used to gain unauthorized access to the network.

07/24/2001 16

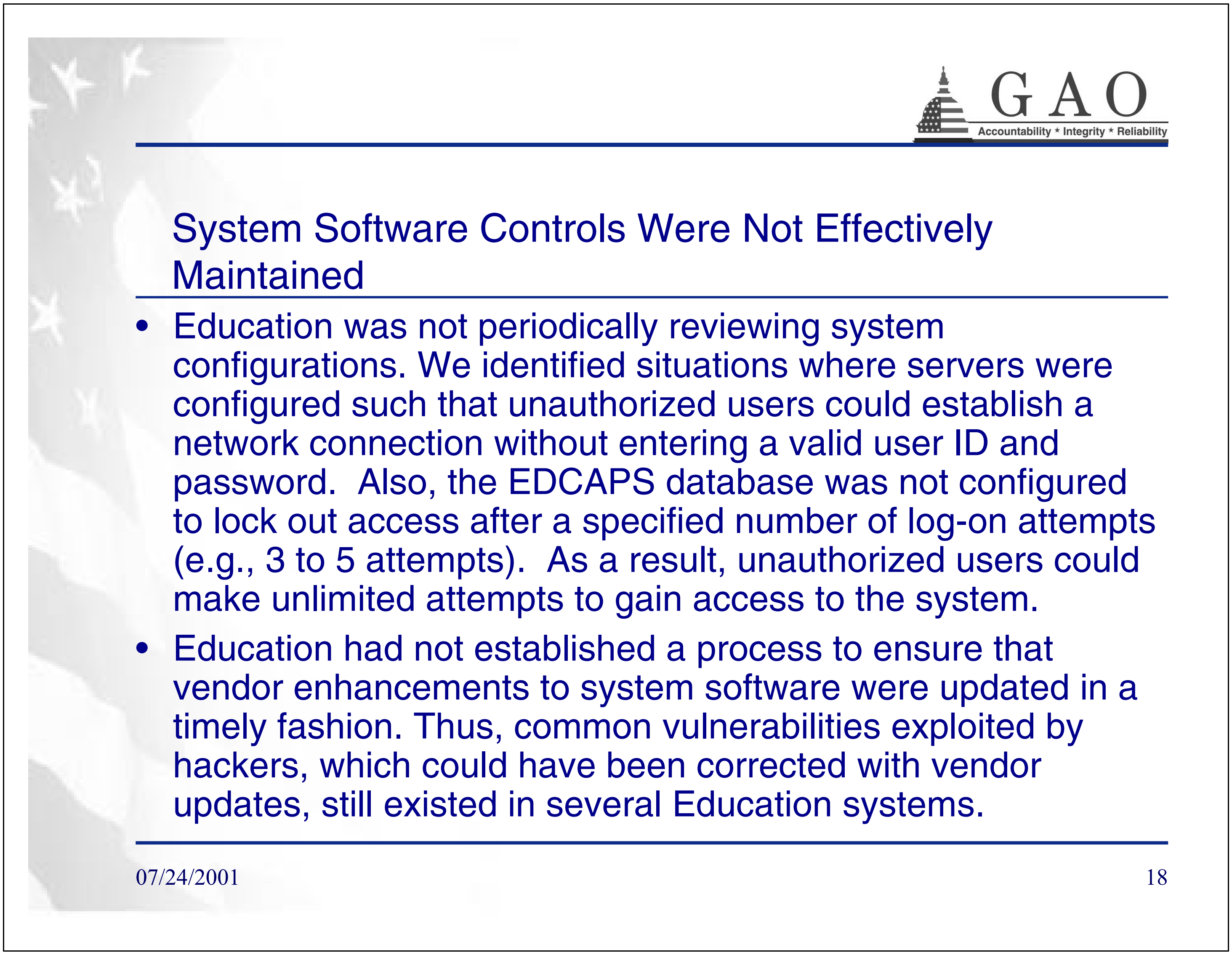


GAO
Accountability * Integrity * Reliability

## Access Authority Was Not Always Appropriately Limited

- About 18,800 users had access privileges that allowed them to modify the database in ways that could result in increased risk to the integrity of EDCAPS information.
- Individual workstations were not adequately secured to prevent access to information maintained on these stations. By connecting to the network without an ID or password, we gained access to files that contained loan information as well as information covered by the Privacy Act, such as students' social security numbers.
- Education had not established compensating controls to ensure that only authorized modifications were made to the network by those users that had administrative access privileges. Such privileges gave them total control of the system that manages the security and password database for Education's computer network.

07/24/2001 17

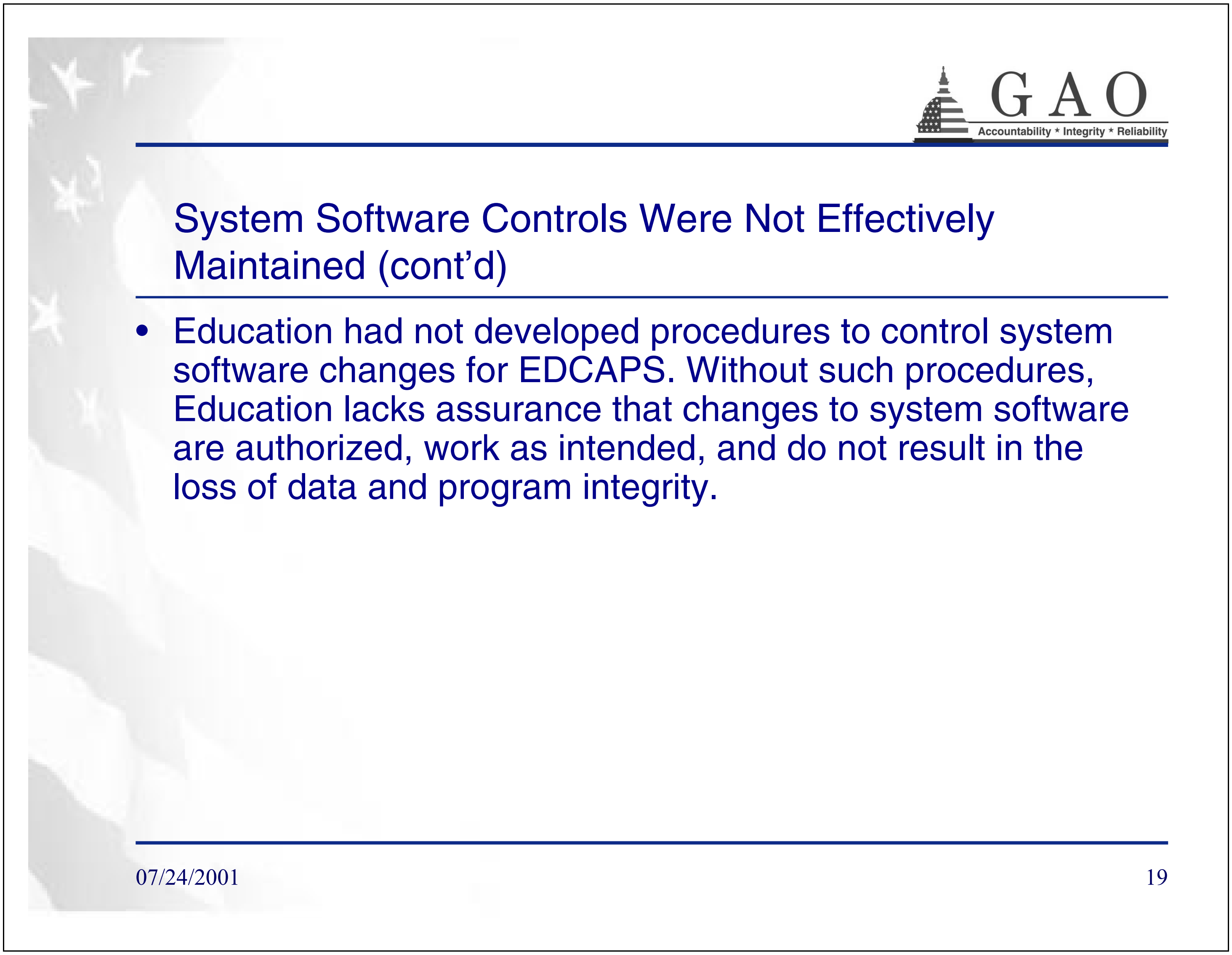


GAO
Accountability * Integrity * Reliability

## System Software Controls Were Not Effectively Maintained

- Education was not periodically reviewing system configurations. We identified situations where servers were configured such that unauthorized users could establish a network connection without entering a valid user ID and password. Also, the EDCAPS database was not configured to lock out access after a specified number of log-on attempts (e.g., 3 to 5 attempts). As a result, unauthorized users could make unlimited attempts to gain access to the system.
- Education had not established a process to ensure that vendor enhancements to system software were updated in a timely fashion. Thus, common vulnerabilities exploited by hackers, which could have been corrected with vendor updates, still existed in several Education systems.

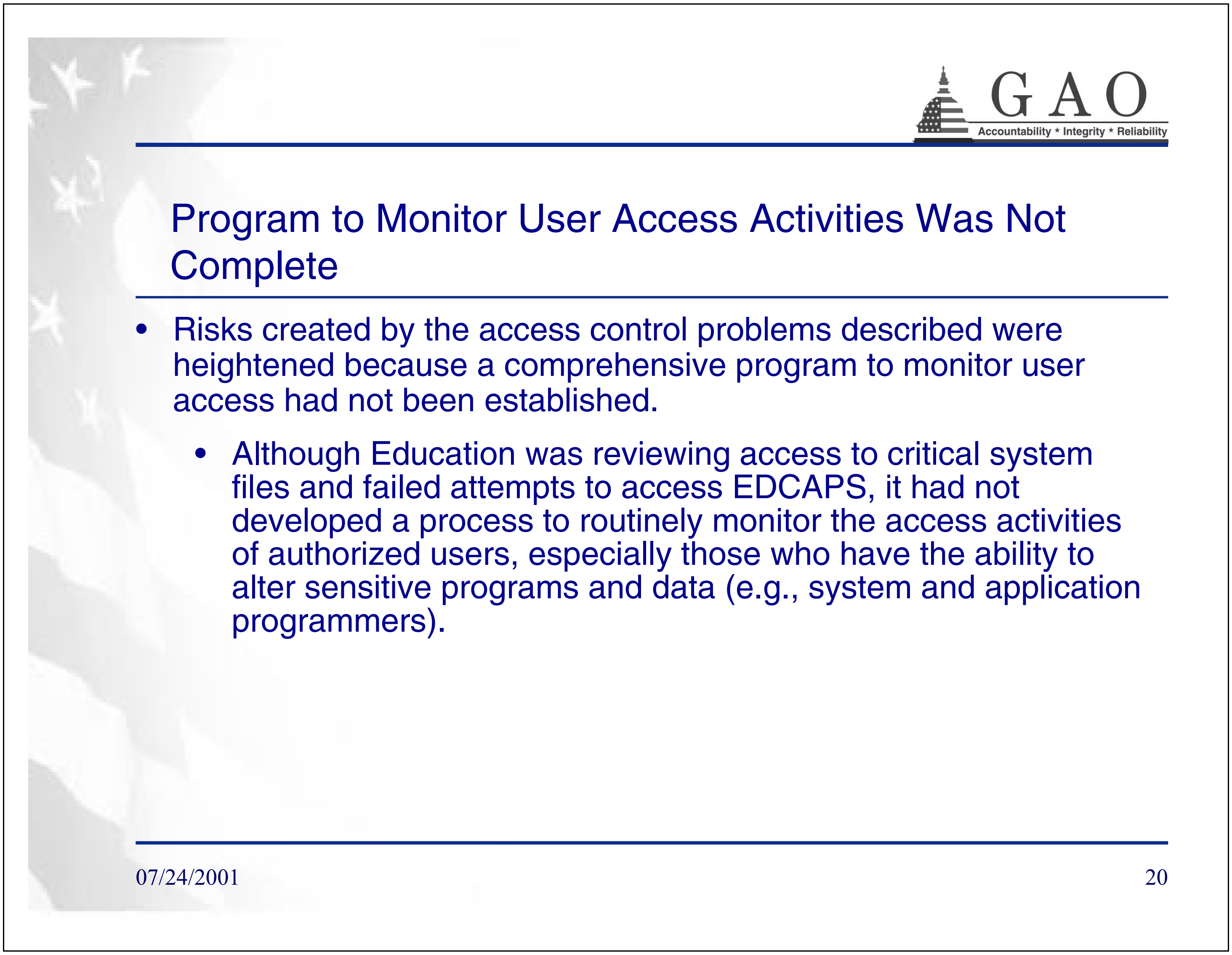
07/24/2001 18



## System Software Controls Were Not Effectively Maintained (cont'd)

- Education had not developed procedures to control system software changes for EDCAPS. Without such procedures, Education lacks assurance that changes to system software are authorized, work as intended, and do not result in the loss of data and program integrity.

07/24/2001 19



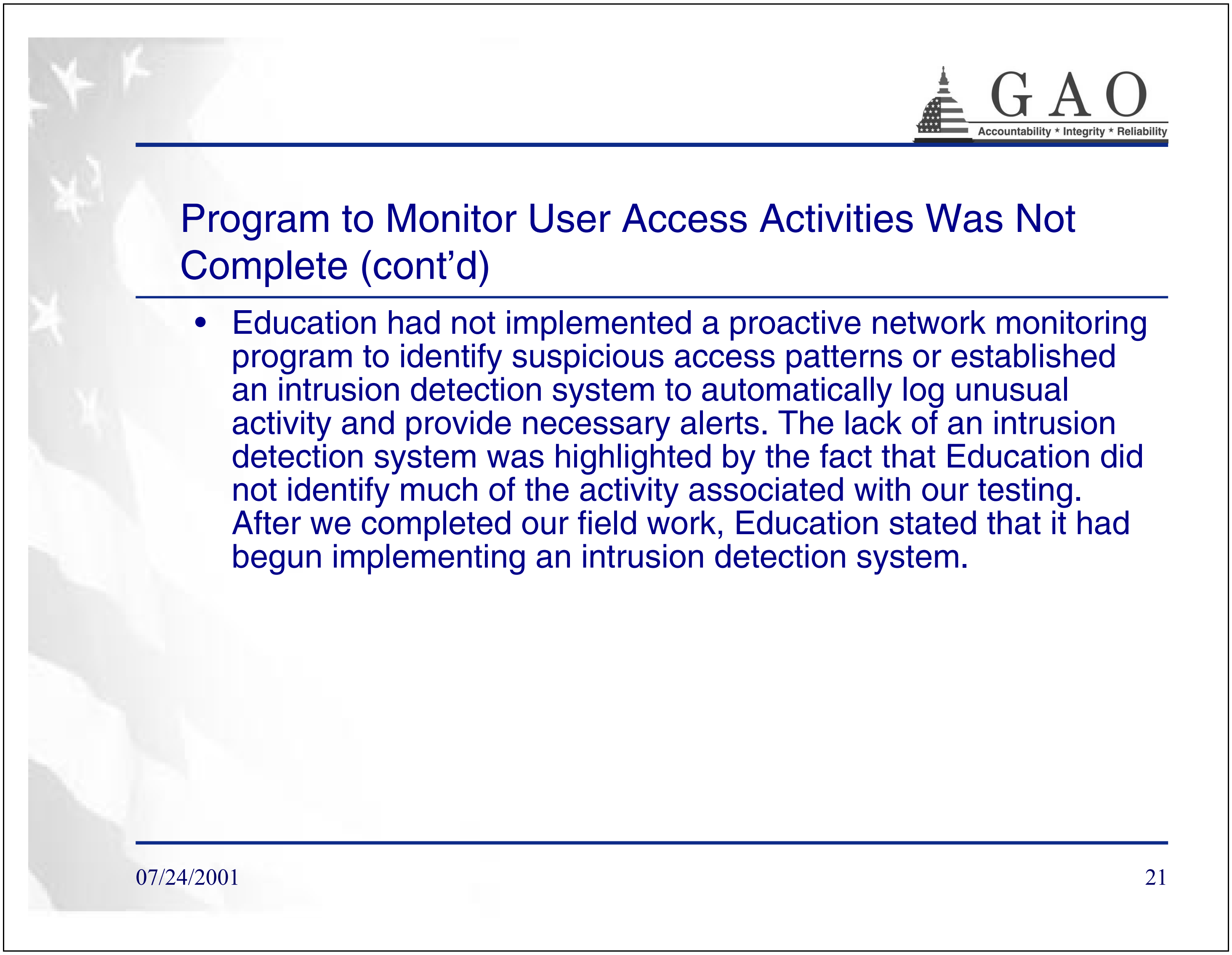
GAO
Accountability * Integrity * Reliability

## Program to Monitor User Access Activities Was Not Complete

- Risks created by the access control problems described were heightened because a comprehensive program to monitor user access had not been established.
    - Although Education was reviewing access to critical system files and failed attempts to access EDCAPS, it had not developed a process to routinely monitor the access activities of authorized users, especially those who have the ability to alter sensitive programs and data (e.g., system and application programmers).

07/24/2001

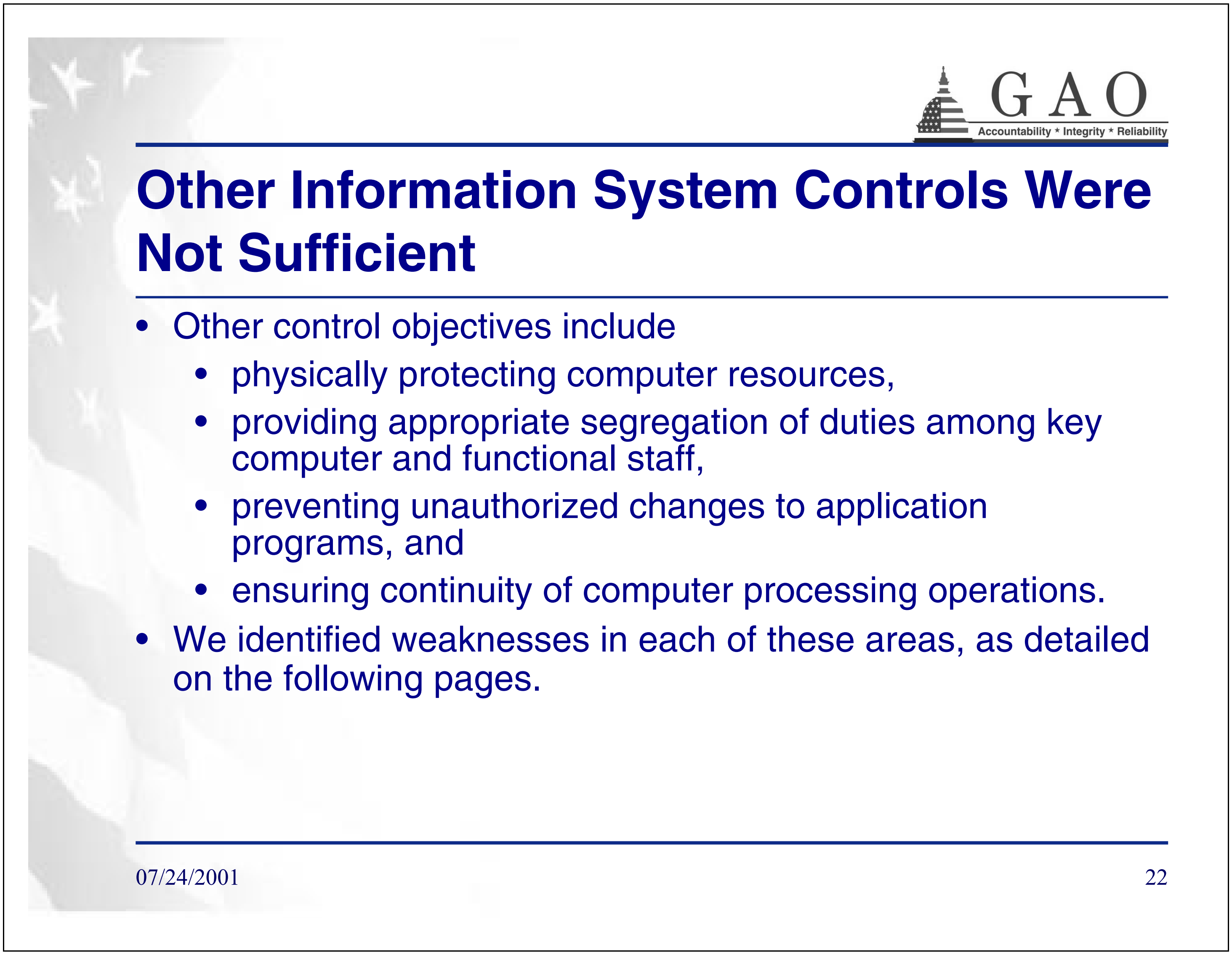
20



## Program to Monitor User Access Activities Was Not Complete (cont'd)

- Education had not implemented a proactive network monitoring program to identify suspicious access patterns or established an intrusion detection system to automatically log unusual activity and provide necessary alerts. The lack of an intrusion detection system was highlighted by the fact that Education did not identify much of the activity associated with our testing. After we completed our field work, Education stated that it had begun implementing an intrusion detection system.

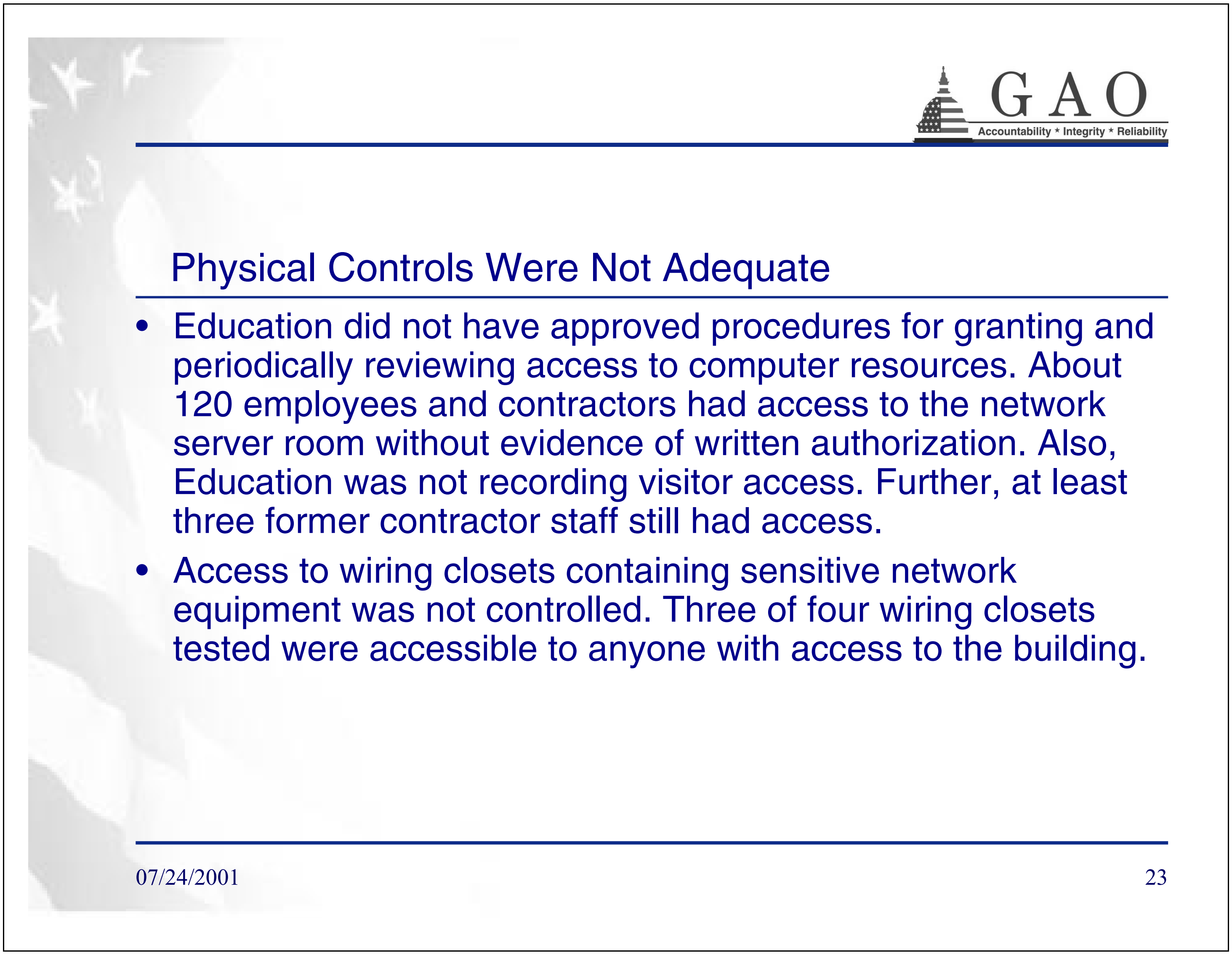
07/24/2001 21



## Other Information System Controls Were Not Sufficient

- Other control objectives include
  - physically protecting computer resources,
  - providing appropriate segregation of duties among key computer and functional staff,
  - preventing unauthorized changes to application programs, and
  - ensuring continuity of computer processing operations.
- We identified weaknesses in each of these areas, as detailed on the following pages.

07/24/2001 22

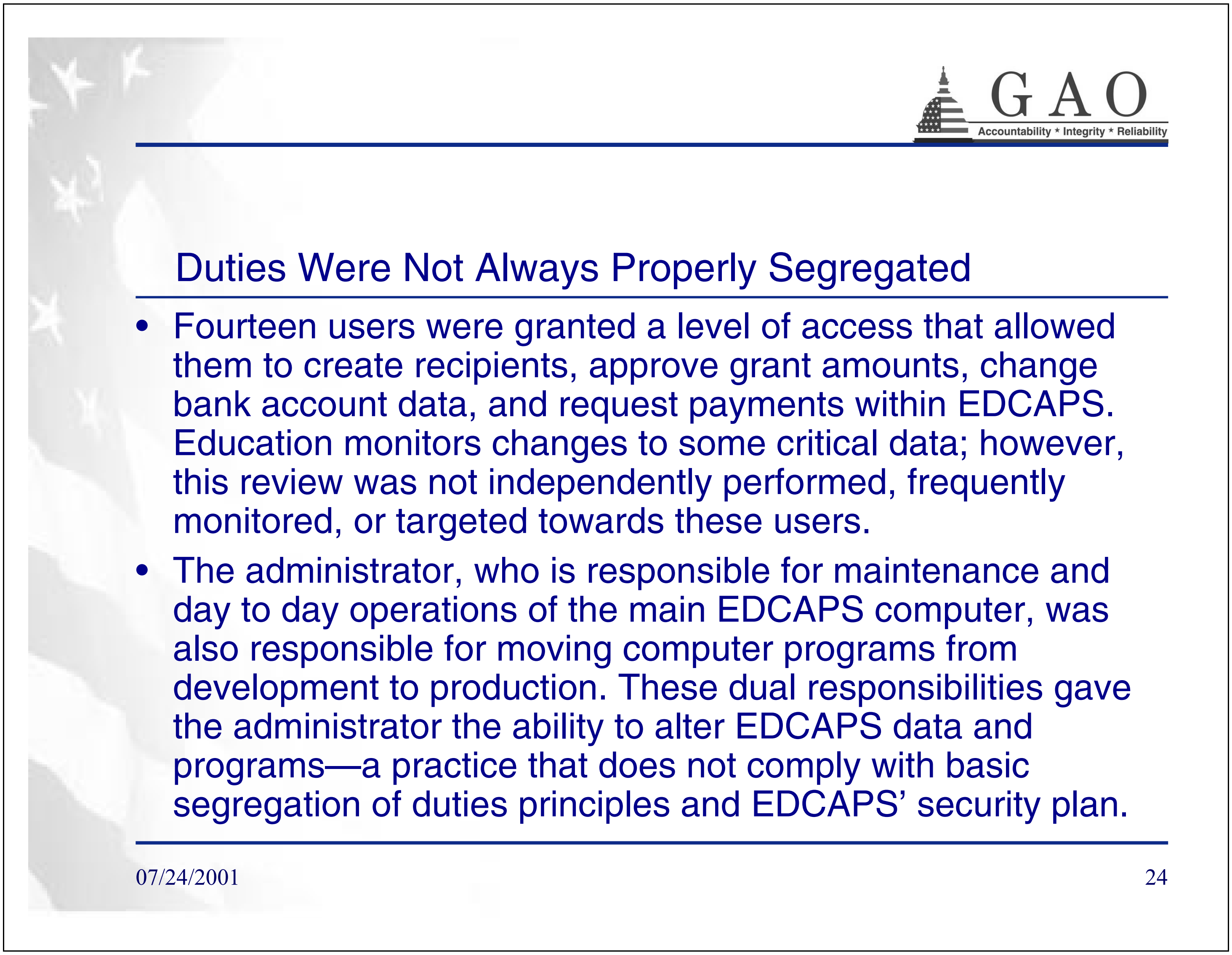


GAO
Accountability * Integrity * Reliability

## Physical Controls Were Not Adequate

- Education did not have approved procedures for granting and periodically reviewing access to computer resources. About 120 employees and contractors had access to the network server room without evidence of written authorization. Also, Education was not recording visitor access. Further, at least three former contractor staff still had access.
- Access to wiring closets containing sensitive network equipment was not controlled. Three of four wiring closets tested were accessible to anyone with access to the building.

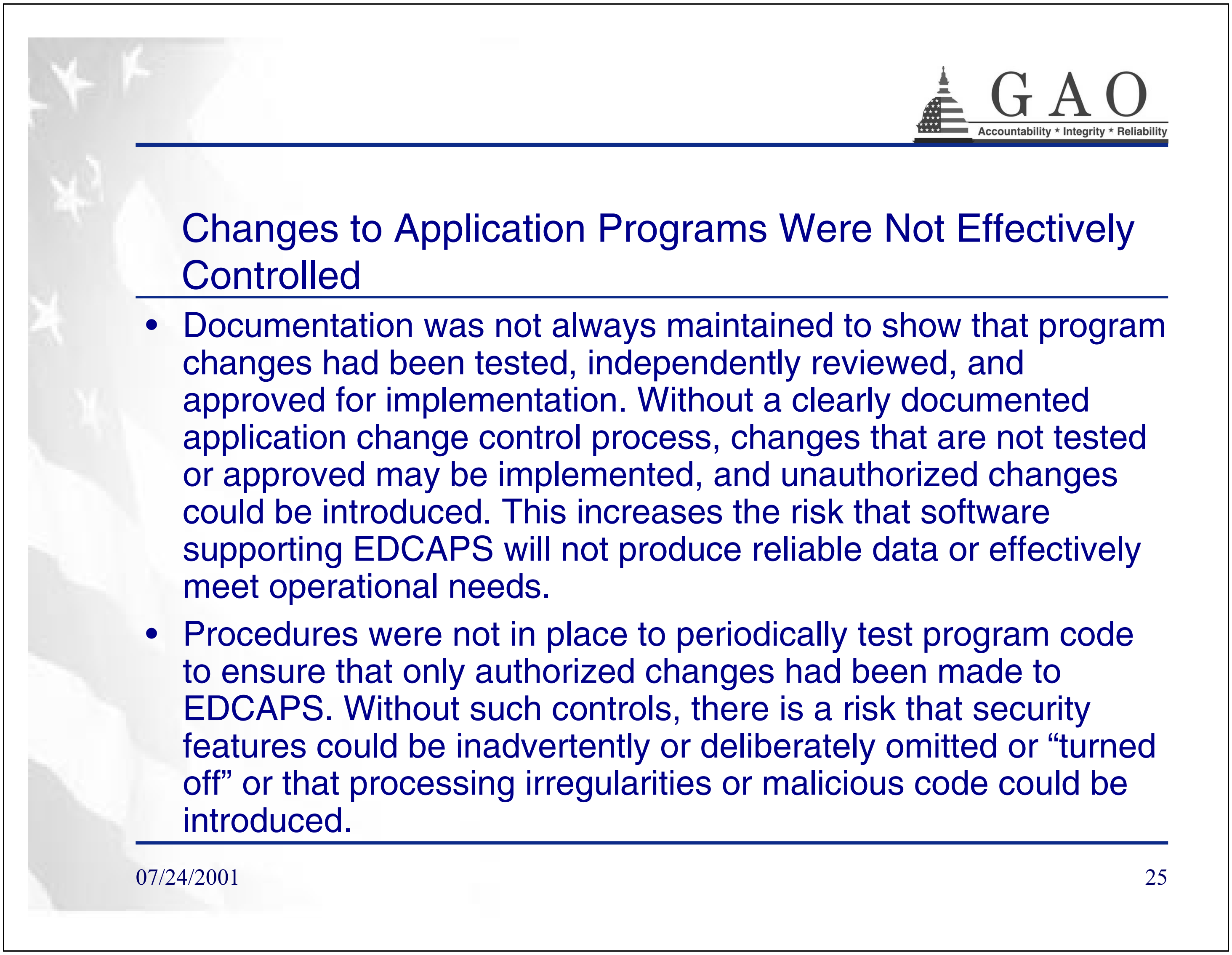
07/24/2001 23



GAO
Accountability * Integrity * Reliability

## Duties Were Not Always Properly Segregated

- Fourteen users were granted a level of access that allowed them to create recipients, approve grant amounts, change bank account data, and request payments within EDCAPS. Education monitors changes to some critical data; however, this review was not independently performed, frequently monitored, or targeted towards these users.
- The administrator, who is responsible for maintenance and day to day operations of the main EDCAPS computer, was also responsible for moving computer programs from development to production. These dual responsibilities gave the administrator the ability to alter EDCAPS data and programs—a practice that does not comply with basic segregation of duties principles and EDCAPS' security plan.

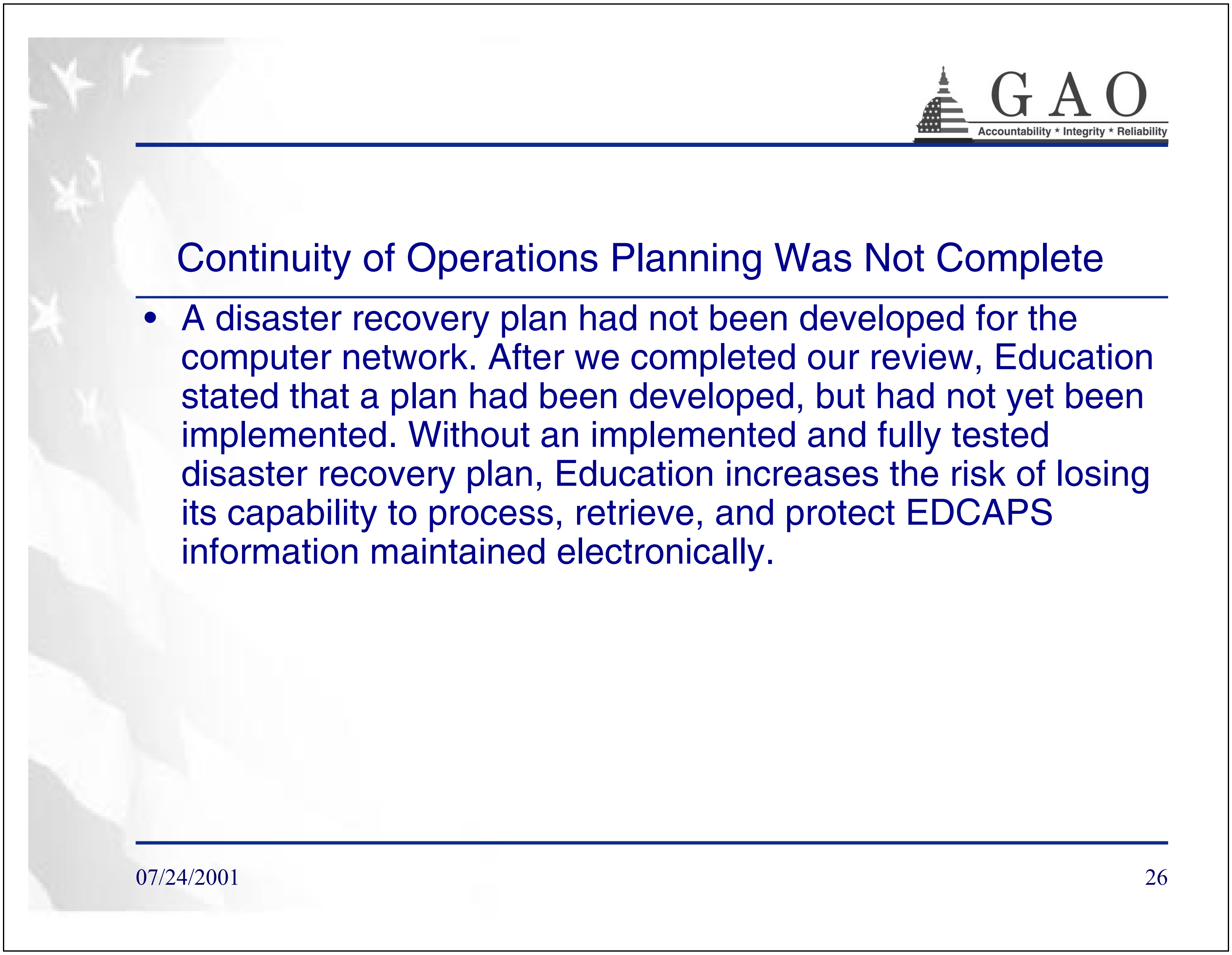


GAO
Accountability * Integrity * Reliability

## Changes to Application Programs Were Not Effectively Controlled

- Documentation was not always maintained to show that program changes had been tested, independently reviewed, and approved for implementation. Without a clearly documented application change control process, changes that are not tested or approved may be implemented, and unauthorized changes could be introduced. This increases the risk that software supporting EDCAPS will not produce reliable data or effectively meet operational needs.
- Procedures were not in place to periodically test program code to ensure that only authorized changes had been made to EDCAPS. Without such controls, there is a risk that security features could be inadvertently or deliberately omitted or "turned off" or that processing irregularities or malicious code could be introduced.

07/24/2001 25

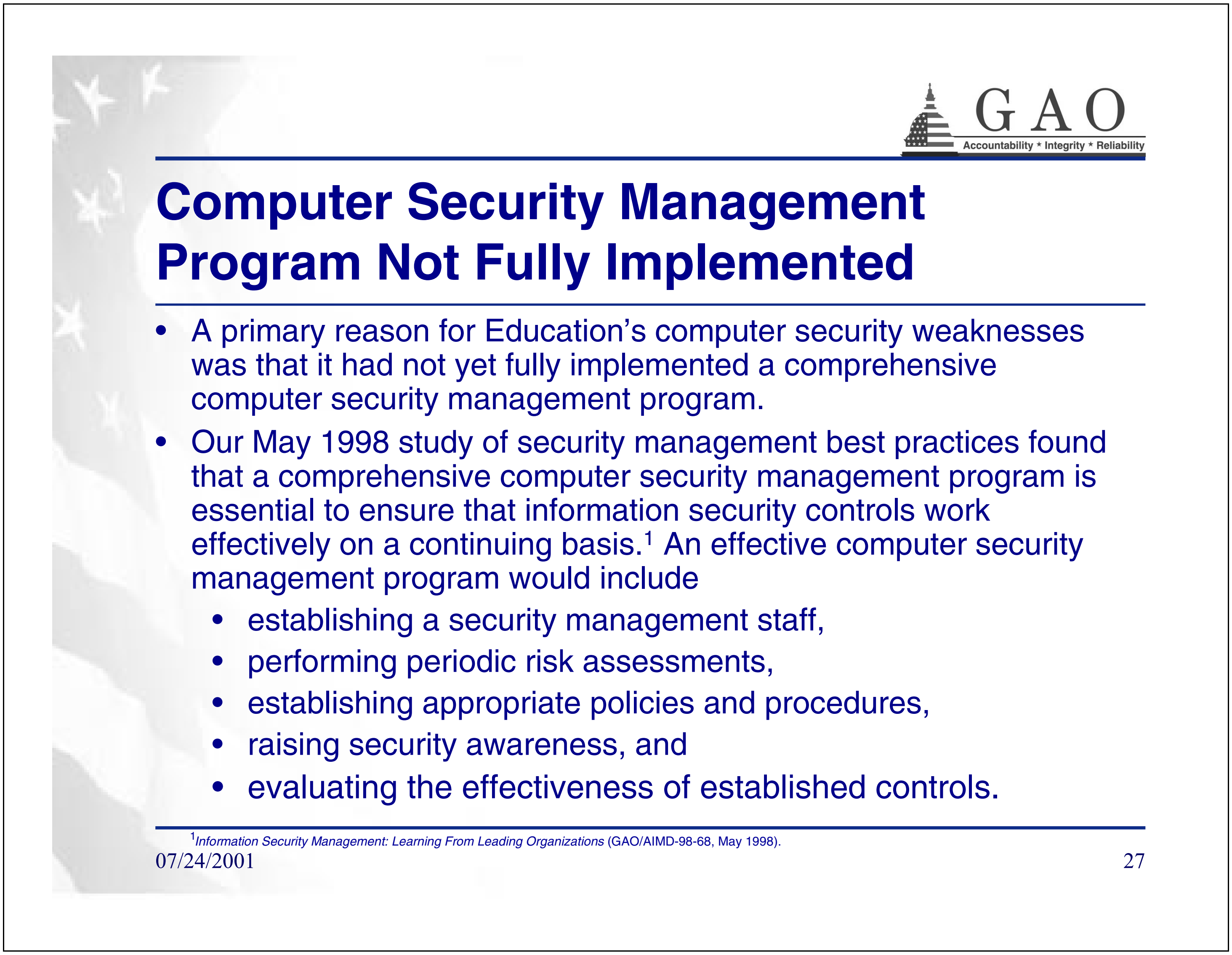


GAO
Accountability * Integrity * Reliability

## Continuity of Operations Planning Was Not Complete

- A disaster recovery plan had not been developed for the computer network. After we completed our review, Education stated that a plan had been developed, but had not yet been implemented. Without an implemented and fully tested disaster recovery plan, Education increases the risk of losing its capability to process, retrieve, and protect EDCAPS information maintained electronically.

07/24/2001 26



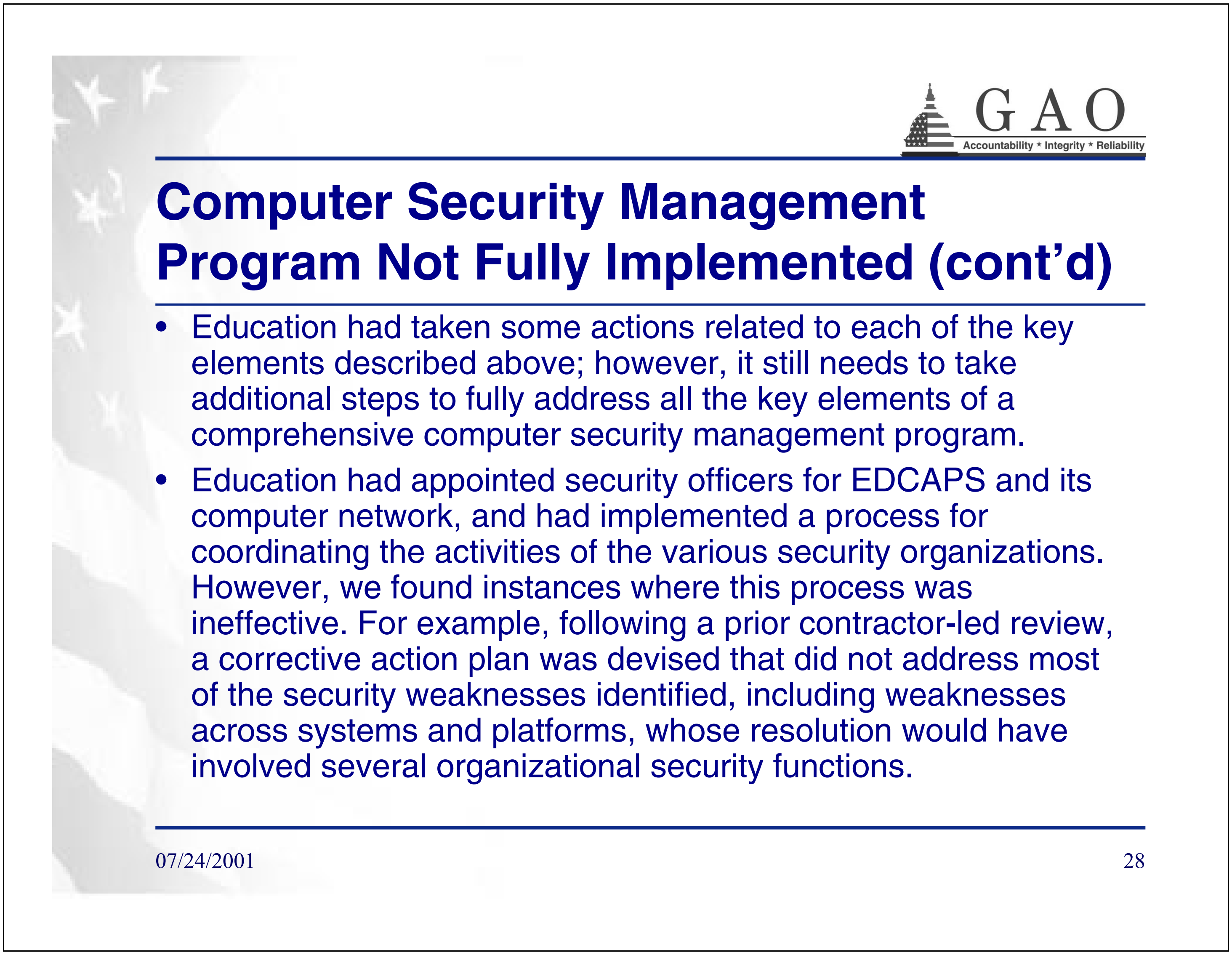
GAO
Accountability * Integrity * Reliability

# Computer Security Management Program Not Fully Implemented

- A primary reason for Education's computer security weaknesses was that it had not yet fully implemented a comprehensive computer security management program.
- Our May 1998 study of security management best practices found that a comprehensive computer security management program is essential to ensure that information security controls work effectively on a continuing basis.[1] An effective computer security management program would include
  - establishing a security management staff,
  - performing periodic risk assessments,
  - establishing appropriate policies and procedures,
  - raising security awareness, and
  - evaluating the effectiveness of established controls.

[1] *Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68, May 1998).

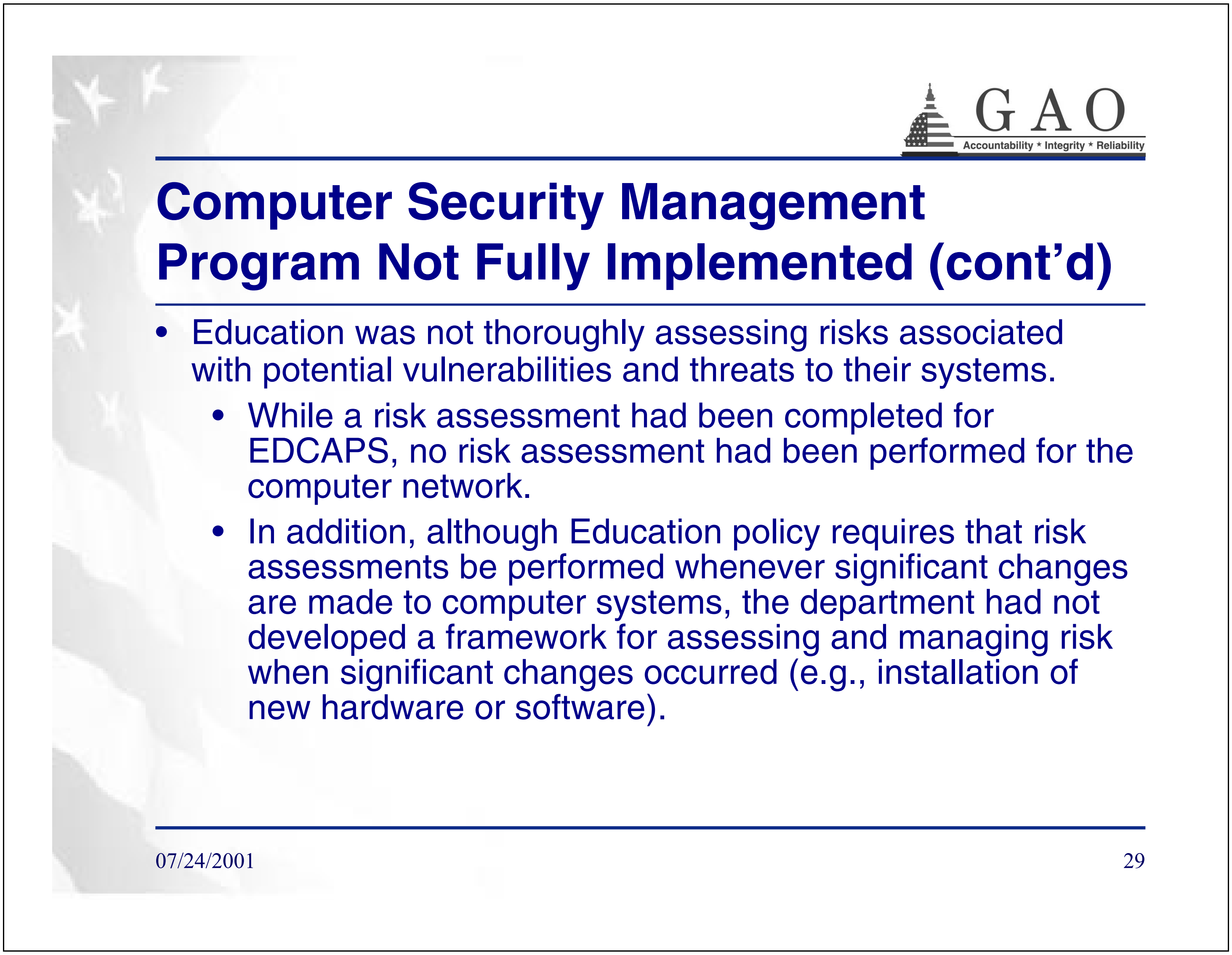
07/24/2001 27



## Computer Security Management Program Not Fully Implemented (cont'd)

- Education had taken some actions related to each of the key elements described above; however, it still needs to take additional steps to fully address all the key elements of a comprehensive computer security management program.
- Education had appointed security officers for EDCAPS and its computer network, and had implemented a process for coordinating the activities of the various security organizations. However, we found instances where this process was ineffective. For example, following a prior contractor-led review, a corrective action plan was devised that did not address most of the security weaknesses identified, including weaknesses across systems and platforms, whose resolution would have involved several organizational security functions.

07/24/2001 28

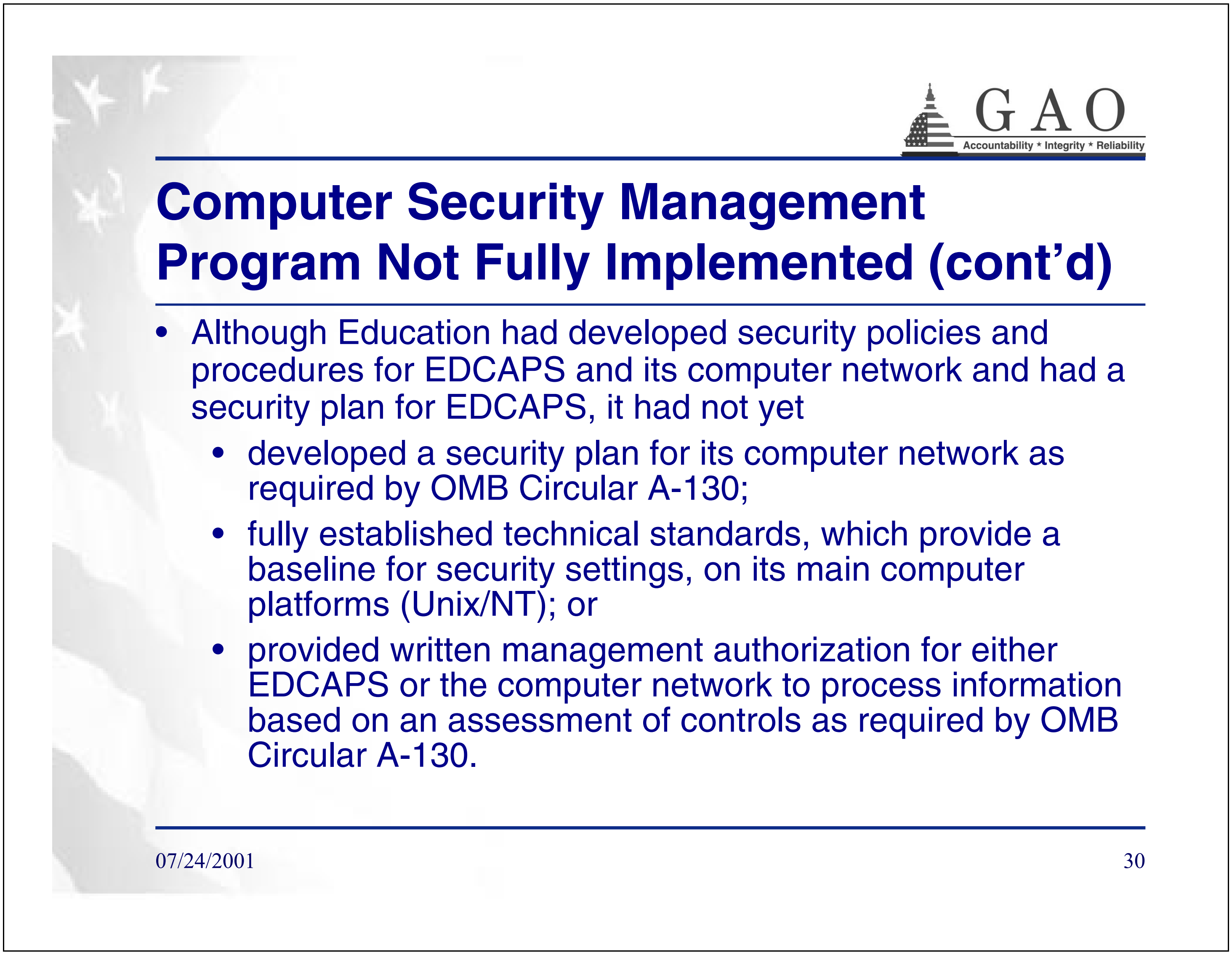


GAO
Accountability * Integrity * Reliability

## Computer Security Management Program Not Fully Implemented (cont'd)

- Education was not thoroughly assessing risks associated with potential vulnerabilities and threats to their systems.
  - While a risk assessment had been completed for EDCAPS, no risk assessment had been performed for the computer network.
  - In addition, although Education policy requires that risk assessments be performed whenever significant changes are made to computer systems, the department had not developed a framework for assessing and managing risk when significant changes occurred (e.g., installation of new hardware or software).

07/24/2001 29

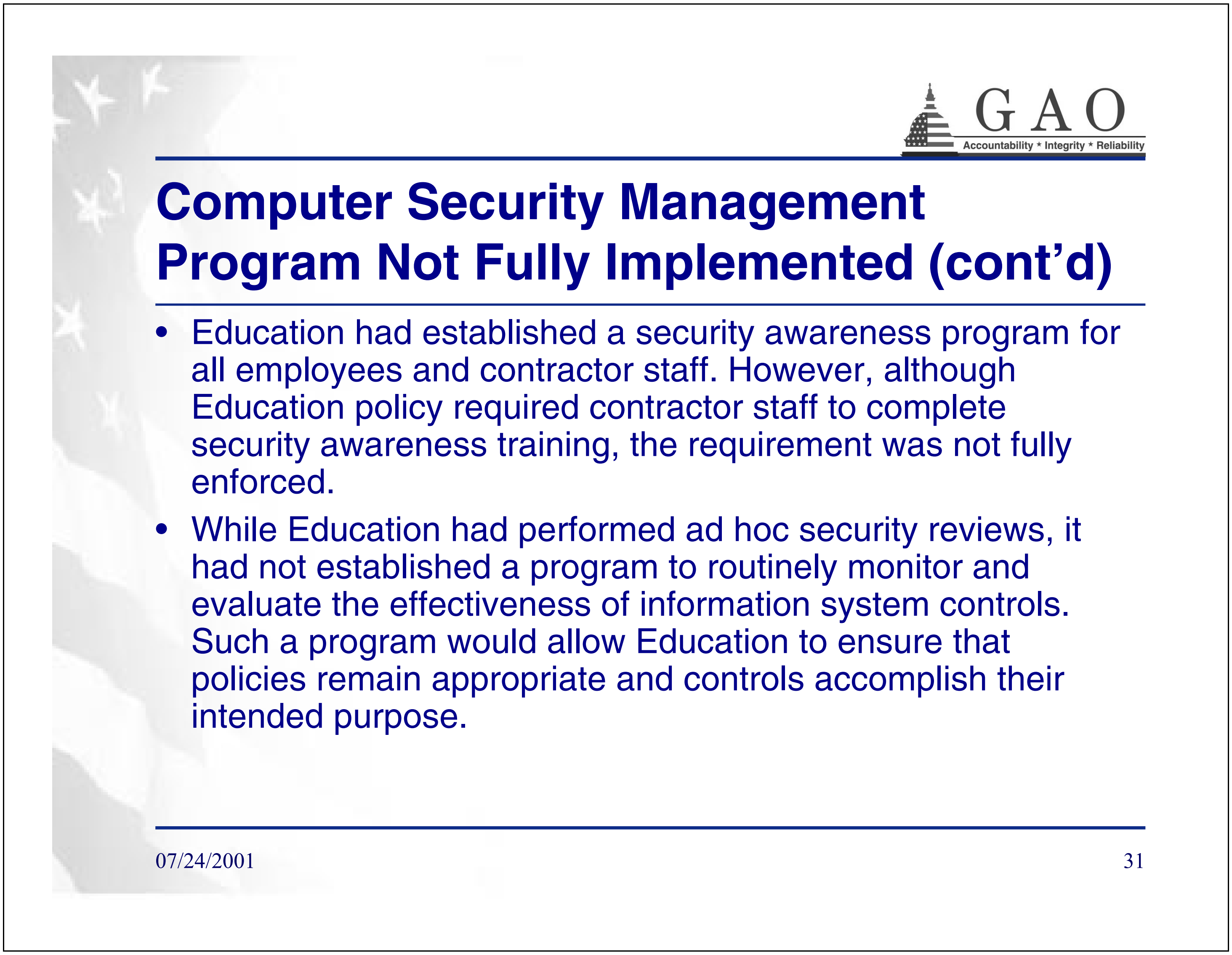


GAO
Accountability * Integrity * Reliability

## Computer Security Management Program Not Fully Implemented (cont'd)

- Although Education had developed security policies and procedures for EDCAPS and its computer network and had a security plan for EDCAPS, it had not yet
  - developed a security plan for its computer network as required by OMB Circular A-130;
  - fully established technical standards, which provide a baseline for security settings, on its main computer platforms (Unix/NT); or
  - provided written management authorization for either EDCAPS or the computer network to process information based on an assessment of controls as required by OMB Circular A-130.

07/24/2001 30

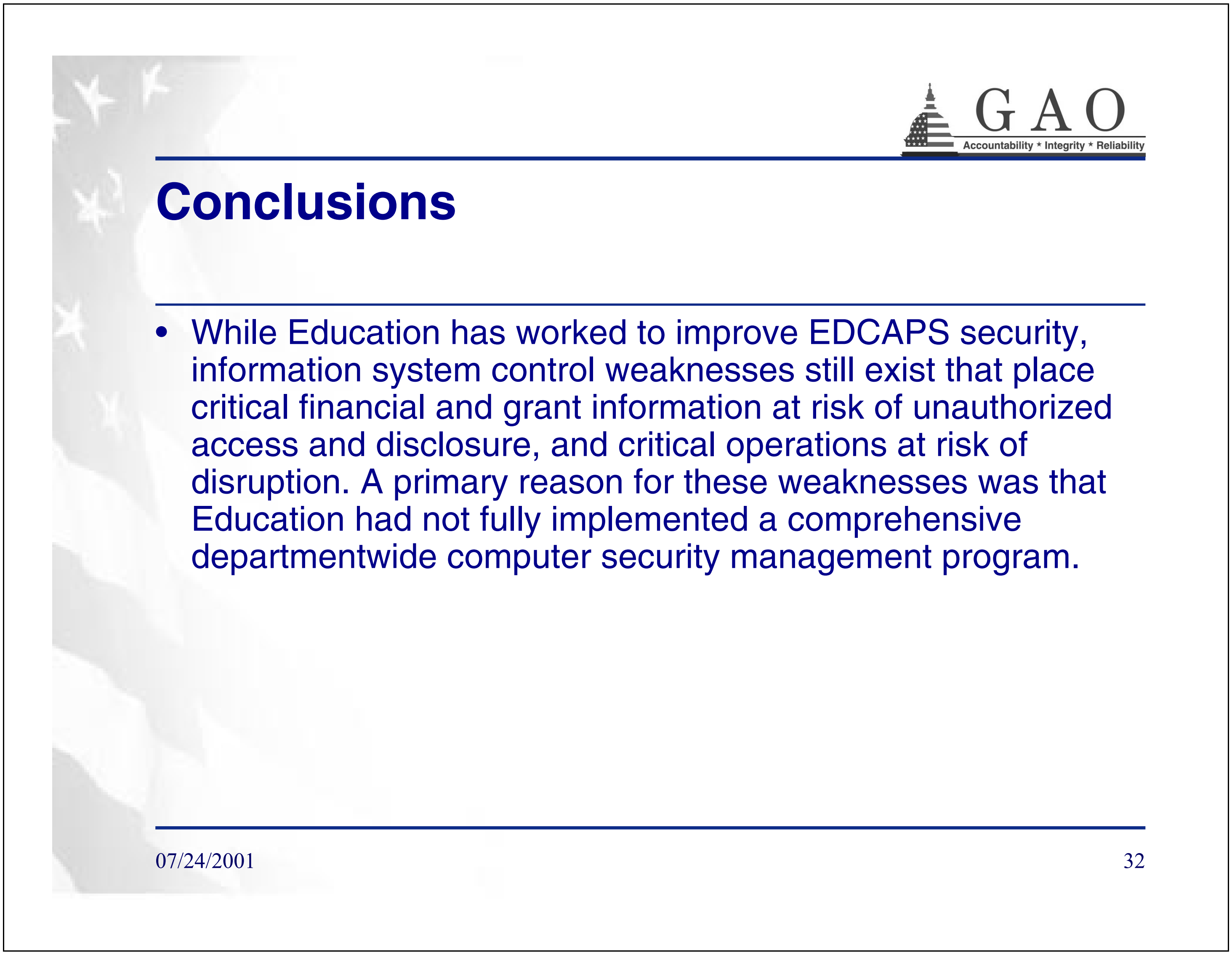


# Computer Security Management Program Not Fully Implemented (cont'd)

- Education had established a security awareness program for all employees and contractor staff. However, although Education policy required contractor staff to complete security awareness training, the requirement was not fully enforced.
- While Education had performed ad hoc security reviews, it had not established a program to routinely monitor and evaluate the effectiveness of information system controls. Such a program would allow Education to ensure that policies remain appropriate and controls accomplish their intended purpose.

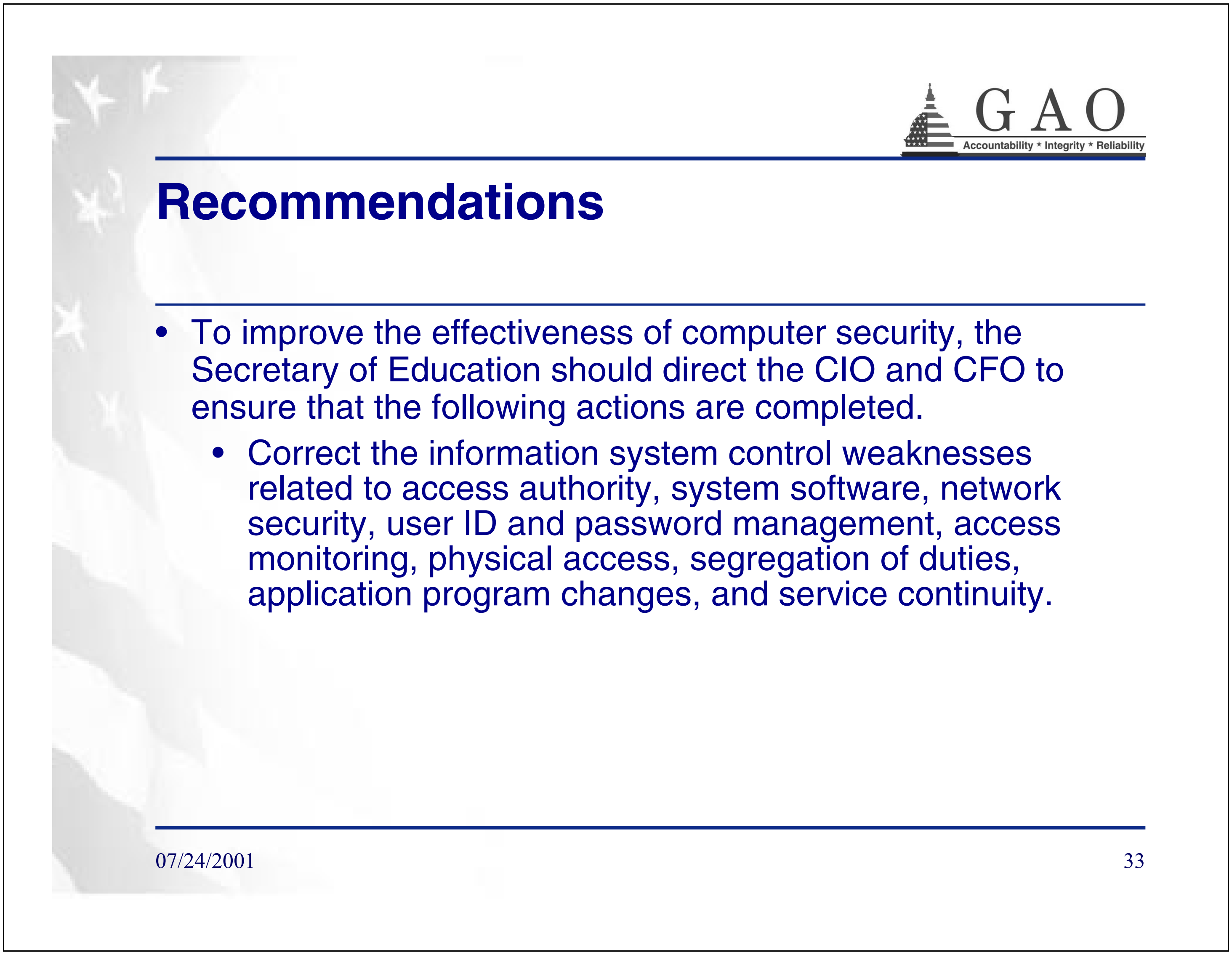
07/24/2001

31



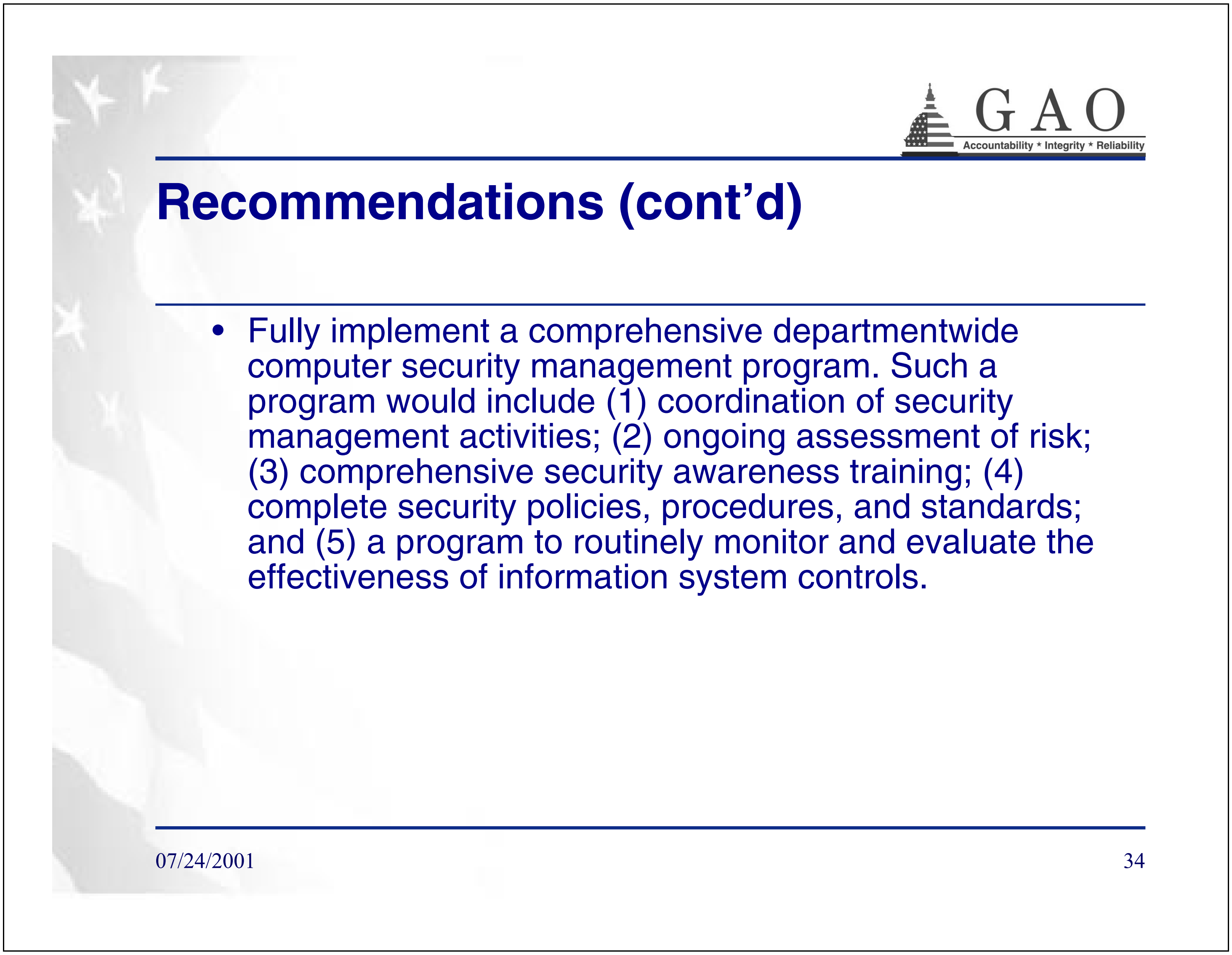
## Conclusions

- While Education has worked to improve EDCAPS security, information system control weaknesses still exist that place critical financial and grant information at risk of unauthorized access and disclosure, and critical operations at risk of disruption. A primary reason for these weaknesses was that Education had not fully implemented a comprehensive departmentwide computer security management program.



# Recommendations

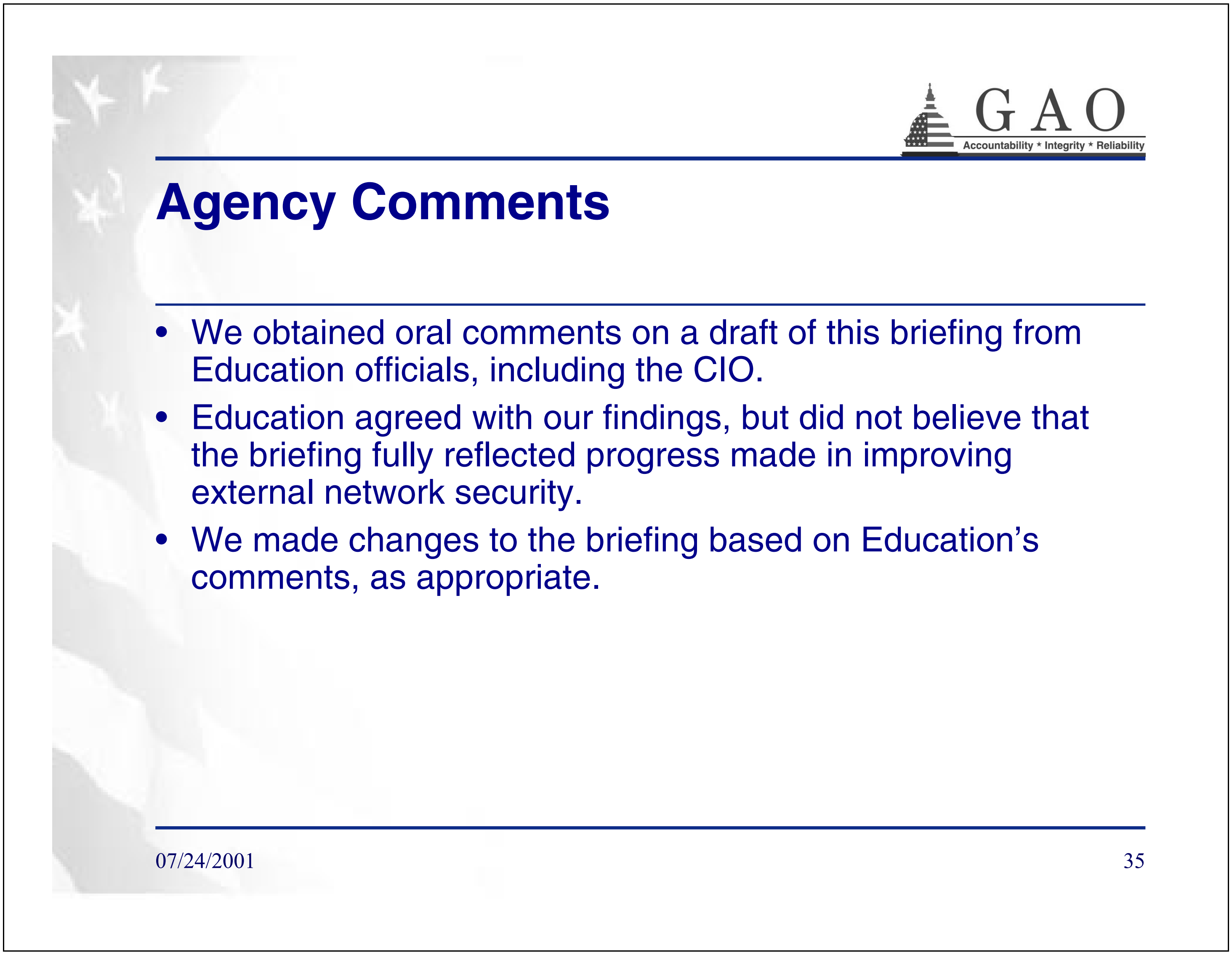
- To improve the effectiveness of computer security, the Secretary of Education should direct the CIO and CFO to ensure that the following actions are completed.
    - Correct the information system control weaknesses related to access authority, system software, network security, user ID and password management, access monitoring, physical access, segregation of duties, application program changes, and service continuity.



## Recommendations (cont'd)

- Fully implement a comprehensive departmentwide computer security management program. Such a program would include (1) coordination of security management activities; (2) ongoing assessment of risk; (3) comprehensive security awareness training; (4) complete security policies, procedures, and standards; and (5) a program to routinely monitor and evaluate the effectiveness of information system controls.

07/24/2001 34



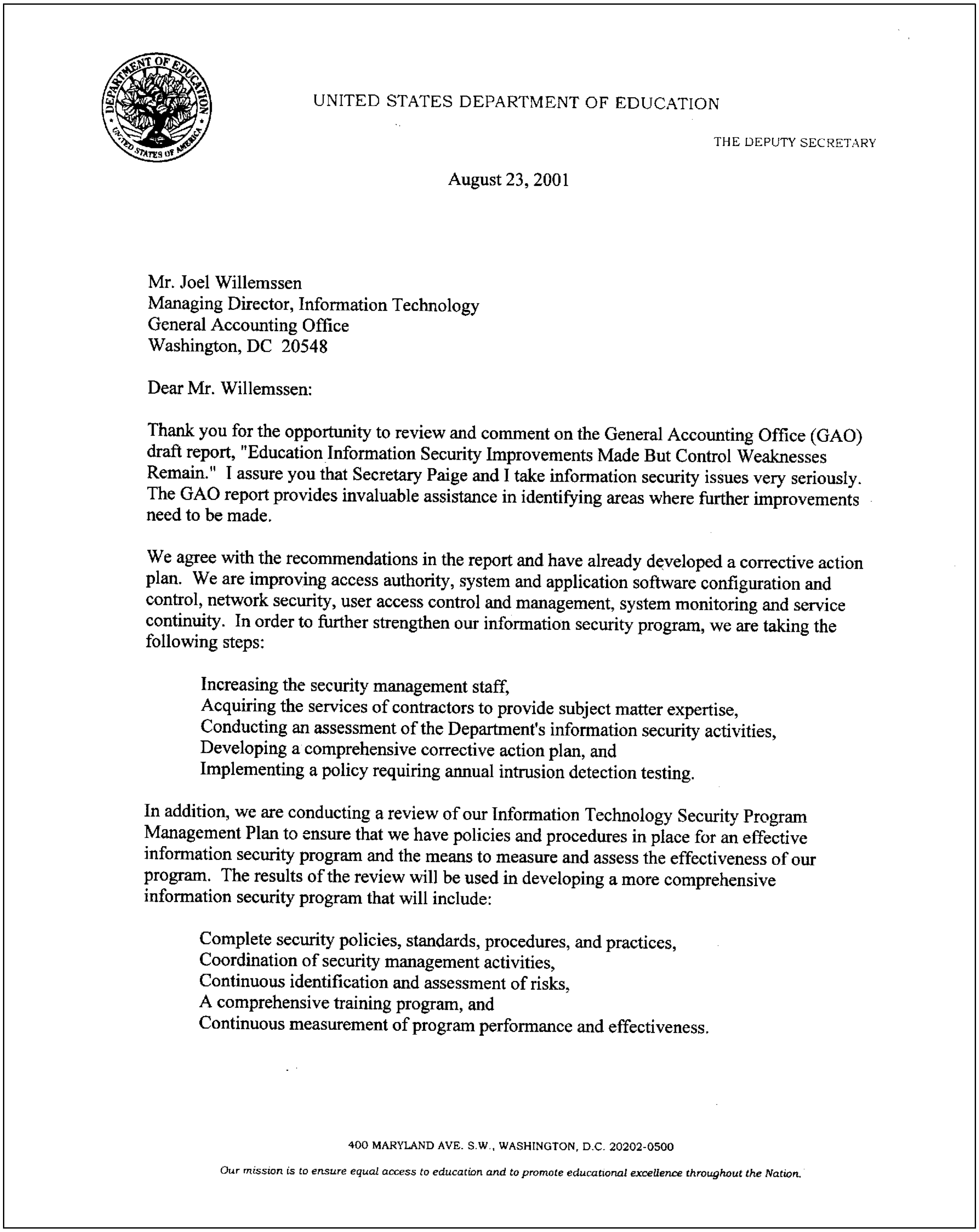
GAO
Accountability * Integrity * Reliability

## Agency Comments

- We obtained oral comments on a draft of this briefing from Education officials, including the CIO.
- Education agreed with our findings, but did not believe that the briefing fully reflected progress made in improving external network security.
- We made changes to the briefing based on Education's comments, as appropriate.

07/24/2001 35

# Agency Comments From the Department of Education



UNITED STATES DEPARTMENT OF EDUCATION

THE DEPUTY SECRETARY

August 23, 2001

Mr. Joel Willemssen
Managing Director, Information Technology
General Accounting Office
Washington, DC 20548

Dear Mr. Willemssen:

Thank you for the opportunity to review and comment on the General Accounting Office (GAO) draft report, "Education Information Security Improvements Made But Control Weaknesses Remain." I assure you that Secretary Paige and I take information security issues very seriously. The GAO report provides invaluable assistance in identifying areas where further improvements need to be made.

We agree with the recommendations in the report and have already developed a corrective action plan. We are improving access authority, system and application software configuration and control, network security, user access control and management, system monitoring and service continuity. In order to further strengthen our information security program, we are taking the following steps:

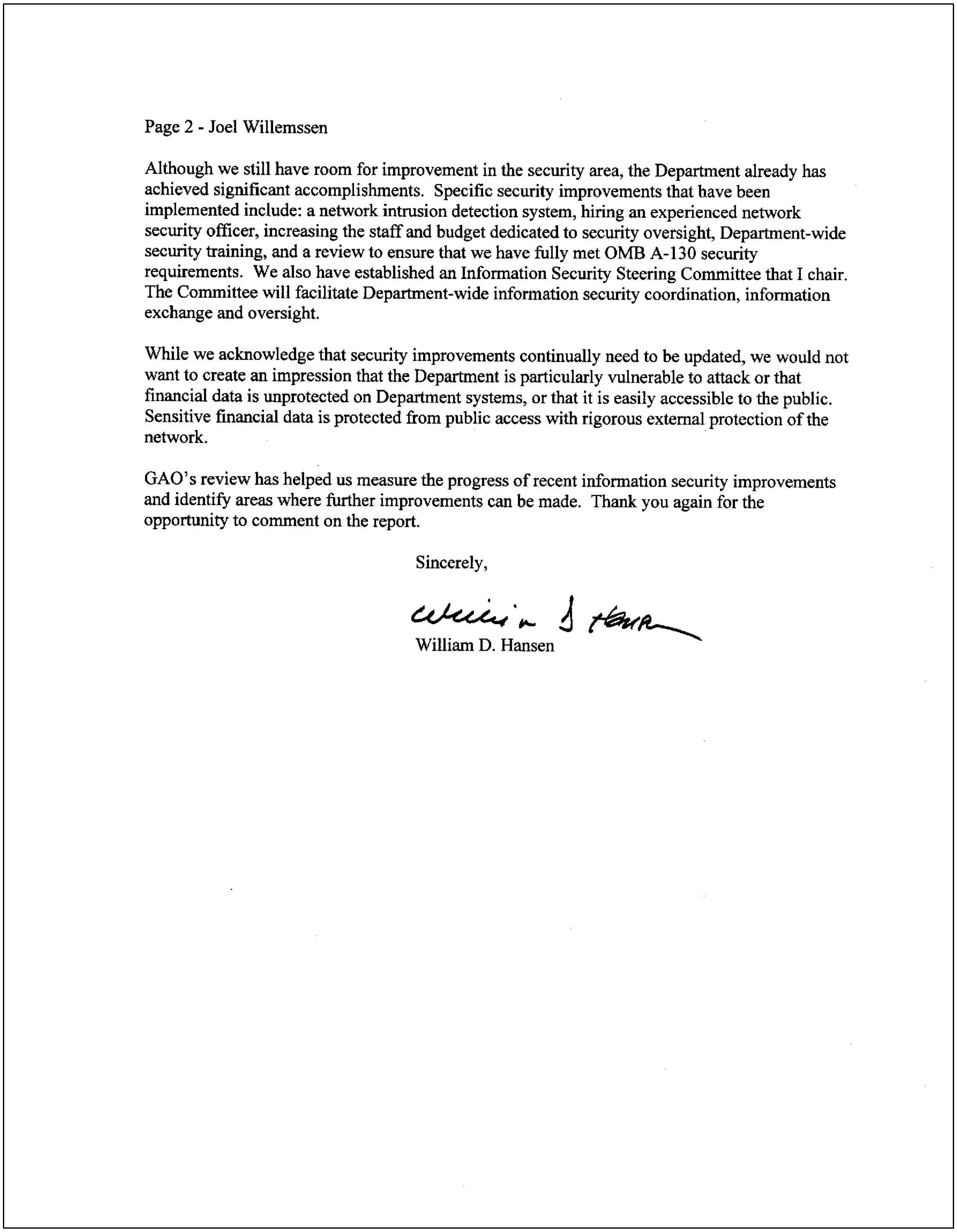
Increasing the security management staff,
Acquiring the services of contractors to provide subject matter expertise,
Conducting an assessment of the Department's information security activities,
Developing a comprehensive corrective action plan, and
Implementing a policy requiring annual intrusion detection testing.

In addition, we are conducting a review of our Information Technology Security Program Management Plan to ensure that we have policies and procedures in place for an effective information security program and the means to measure and assess the effectiveness of our program. The results of the review will be used in developing a more comprehensive information security program that will include:

Complete security policies, standards, procedures, and practices,
Coordination of security management activities,
Continuous identification and assessment of risks,
A comprehensive training program, and
Continuous measurement of program performance and effectiveness.

400 MARYLAND AVE. S.W., WASHINGTON, D.C. 20202-0500

*Our mission is to ensure equal access to education and to promote educational excellence throughout the Nation.*



Page 2 - Joel Willemssen

Although we still have room for improvement in the security area, the Department already has achieved significant accomplishments. Specific security improvements that have been implemented include: a network intrusion detection system, hiring an experienced network security officer, increasing the staff and budget dedicated to security oversight, Department-wide security training, and a review to ensure that we have fully met OMB A-130 security requirements. We also have established an Information Security Steering Committee that I chair. The Committee will facilitate Department-wide information security coordination, information exchange and oversight.

While we acknowledge that security improvements continually need to be updated, we would not want to create an impression that the Department is particularly vulnerable to attack or that financial data is unprotected on Department systems, or that it is easily accessible to the public. Sensitive financial data is protected from public access with rigorous external protection of the network.

GAO's review has helped us measure the progress of recent information security improvements and identify areas where further improvements can be made. Thank you again for the opportunity to comment on the report.

Sincerely,

William D. Hansen

# GAO Contact and Staff Acknowledgments

## GAO Contact

Dave Irvin, (214) 777-5716

## Acknowledgments

In addition to the person named above, Edward Alexander, West Coile, Debra Conner, Kristi Dorsey, Brian Howe, Jeffrey Knott, Harold Lewis, Suzanne Lightman, Duc Ngo, Norman Poage, Eugene Stevens, and Charles Vrabel made key contributions to this report.

## Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:
U.S. General Accounting Office
P.O. Box 37050
Washington, DC  20013

Orders by visiting:
Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

Orders by Internet:
For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

## To Report Fraud, Waste, or Abuse in Federal Programs

Contact one:

- Web site: http://www.gao.gov/fraudnet/fraudnet.htm
- e-mail: fraudnet@gao.gov
- 1-800-424-5454 (automated answering system)

PRINTED ON ♻ RECYCLED PAPER

[redacted]