United States General Accounting Office

GAO

Report to Congressional Requesters

June 2002

INFORMATION TECHNOLOGY

DOD Needs to Improve Process for Ensuring Interoperability of Telecommunications Switches

GAO-02-681

GAO
Accountability★Integrity★Reliability

Highlights

INFORMATION TECHNOLOGY DOD Needs to Improve Process for Ensuring Interoperability of Telecommunications Switches

Highlights of GAO-02-681, a report to Congressional Requesters.

Why GAO Did This Study

The Department of Defense (DOD) requires that its communications systems be interoperable: that is, that they work together seamlessly so that the right information gets to the right people at the right time. GAO was asked to examine DOD's process for certifying and authorizing interoperability; how the process was being applied, including whether contracting laws and regulations have been violated; and the impact of DOD's application of the process on competition.

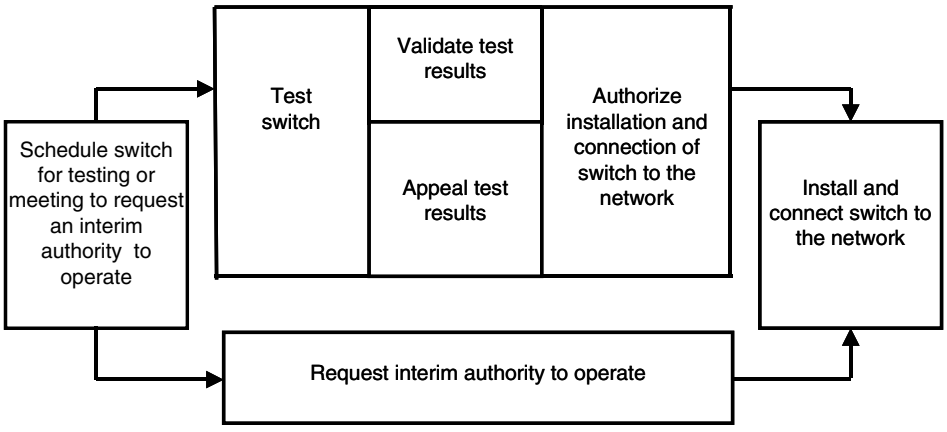
What GAO Found

DOD does not have a well-defined process, including clear requirements, for certifying and authorizing telecommunications (telecom) switches. DOD's process is not fully documented, current, or complete. Additionally, the process lacks an effective enforcement mechanism. As a result, DOD is increasing the risk that its certification and authorization process will be applied inconsistently and that the department's telecommunications will experience future interoperability problems. DOD attributed these weaknesses to the fact that the process is relatively new and still evolving.

Further, DOD has not applied its telecom switch certification and authorization process consistently across vendors, and it has in some cases violated the department's interoperability policy. For example, while the Army required one vendor to remove its uncertified switch from one location, it allowed another vendor to install its uncertified switch at two locations, which violated the policy. However, in reviewing this and other examples of DOD's application of the interoperability certification and authorization process, GAO did not find that contracting laws and regulations had been violated.

Moreover, DOD's application of its telecom switch certification and authorization process is influencing vendors' plans for competing for the department's business. For example, one of five vendors we interviewed stated that it has stopped doing business with DOD for economic reasons (the costs associated with testing and certification exceed potential business opportunities). Another vendor stated that it is reconsidering its participation because of the department's inconsistent application of the process. Within the department itself, positions are mixed regarding the impact of the process on DOD's goal to encourage vendor competition.

Overview of department's process for certifying and authorizing telecom switches. Each of the seven process areas consists of multiple steps and decision points.



Source: GAO analysis of DOD-supplied evidence.

What GAO Recommends

To assist DOD in achieving its goal of ensuring network interoperability, GAO recommends short- and long-term actions that focus on the department's need to revise its switch certification and authorization process to ensure that it is complete, current, transparent to stakeholders, and enforceable.

DOD concurred with the recommendations and stated that their implementation should improve the department's certification process for telecom switches.

Contents

Letter

1

Recommendations for Executive Action 2
Agency Comments and Our Evaluation 3

Appendixes

Appendix I: Briefing Slides from April 19, 2002, Briefing to Staffs of Senators Helms and Warner 6

Appendix II: Comments from the Department of Defense 93

Appendix III: GAO Contact and Staff Acknowledgments 96
GAO Contact 96
Staff Acknowledgments 96

Abbreviations

C3I	Command, Control, Communications, and Intelligence
DOD	Department of Defense
telecom	telecommunications

GAO
Accountability * Integrity * Reliability

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

June 28, 2002

The Honorable Jesse Helms
The Honorable John Warner
United States Senate

In November 1992, the Department of Defense (DOD) issued a policy requiring systems to be interoperable.[1] In May 2000, the department began to enforce this policy for telecommunications (telecom) switches,[2] requiring them to be tested and certified for interoperability before being installed for operational use within the DOD network. In response to your request, we determined (1) DOD's process for certifying and authorizing the interoperability of telecom switches; (2) how the process is being applied, including whether contracting laws and regulations have been violated; and (3) how the process affects vendor competition.

On April 19, 2002, we briefed your staffs on the results of our review. This report transmits to the Secretary of Defense the briefing materials and the recommendations that we specified in the briefing. The full briefing, including our scope and methodology, is reprinted in appendix I. In summary, we made three major points:

- DOD does not have a well-defined process, including clear requirements, for certifying and authorizing telecom switches. DOD's process is not fully documented, current, or complete. Additionally, the process lacks an effective enforcement mechanism. Without a well-defined process and effective enforcement, DOD increases the risk that its certification and authorization process will be applied inconsistently and that the department's telecommunications will experience future interoperability problems. DOD officials attributed the weaknesses to the process being relatively new.

- Second, DOD has not applied its telecom switch certification and authorization process consistently across vendors, and it has in some cases violated policy. For example, while the Army required one vendor to remove its uncertified switch from one location, it allowed another

[1]Interoperability is the ability of systems to work together effectively and efficiently so that the right information gets to the right people at the right time.

[2]Telecom switches are hardware and software designed to send and receive voice, data, and video signals across a network.

vendor to install its uncertified switch at two locations, which violated the department's policy. However, in reviewing this and other examples of DOD's application of the interoperability certification and authorization process, we did not find that contracting laws and regulations had been violated. Again, DOD attributed these inconsistencies to the process being relatively new and still evolving.

- Third, DOD's application of its telecom switch certification and authorization process is influencing vendors' plans for competing for the department's business. One of five vendors we interviewed stated that it has stopped doing business with DOD for economic reasons (i.e., the costs associated with testing and certification exceed potential business opportunities). Another vendor stated that it is reconsidering its participation because of the department's inconsistent application of the process. Within DOD, positions are mixed on the impact of the department's interoperability goal on competition.

Recommendations for Executive Action

To ensure network interoperability and address the potential impact on competition for telecom switch vendors, we recommend that the Secretary of Defense advance the state of maturity of DOD's telecom switch certification and authorization process by directing the Chairman of the Joint Chiefs of Staff, as the DOD authority responsible for the process, to take the following near-term and long-term actions to improve the process.

In the near term,

- use the process flowcharts provided in the following briefing to assist in fully documenting the existing certification and authorization process, and

- make this fully documented process available to DOD and vendor process stakeholders within 60 days.

In the longer term, revise the existing process (including switch requirements) to ensure that it is complete, current, transparent to stakeholders, and enforceable by the Joint Staff, and issue a revised process to all stakeholders within 180 days. In doing so, the Chairman should

- work jointly with the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (C3I), since this organization

is responsible for the interoperability policy and for providing guidance and oversight;

- solicit DOD and vendor input on needed process changes; and
- seek DOD and vendor comments on a draft of the revised process before it is issued in final form.

We also recommend that the Secretary direct the Director of the Defense Information Systems Agency, as the DOD authority responsible for certifying the interoperability of switches, to complete its ongoing inventory of switches installed in the Defense Switched Network. We further recommend that the Secretary direct the Assistant Secretary of Defense for C3I, in collaboration with the Chairman, to use this inventory to assess the level of interoperability risk associated with having uncertified switches on the network and to develop and implement a risk mitigation strategy to address any risks identified.

Agency Comments and Our Evaluation

In written comments on a draft of this report (see appendix II), the Director of Architecture and Interoperability, Office of the Assistant Secretary of Defense for C3I, stated that the department agreed with our recommendations and that implementing the recommendations should improve its certification process for telecommunications switches. The department also described recently completed, ongoing, and planned efforts to address each of the recommendations. The department then stated that it strongly believes that its existing technical approach for certifying known telecommunications switches is sufficient. We do not question this statement because our review focused on DOD's management of its certification process and the implementation of this process. It did not address the technical testing environment and standards for certifying switches.

The department also did not agree with our position that the Army's installation of an uncertified switch both at the Funari and Coleman Barracks in Germany is an example of inconsistent application of existing DOD interoperability policy and procedures. In both of these instances, according to DOD's comments, uncertified switches were only temporarily connected for testing purposes and were not operationally deployed. This comment is inconsistent with the position of officials representing Army's Communications-Electronics Command Systems Management Center, which is responsible for installing and operating these switches. According

to these officials, the switches installed at these two locations were operationally deployed without having the required interim authority to operate or certification. As a result, we did not change the report to reflect this comment.

We are sending copies of this report to the Chairmen and Ranking Minority Members of the Senate Committee on Armed Services; Subcommittee on Defense, Senate Committee on Appropriations; House Committee on Armed Services; and Subcommittee on Defense, House Committee on Appropriations. We are also sending copies to the Director, Office of Management and Budget; the Secretary of Defense; the Secretary of the Army; the Secretary of the Navy; the Secretary of the Air Force; the Assistant Secretary of Defense for C3I/Chief Information Officer; the Joint Staff Director for Command, Control, Communications, and Computer Systems; the Director of Interoperability for the Under Secretary of Defense for Acquisition, Technology, and Logistics; and the Director of the Defense Information Systems Agency. We will also make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

Should you or your staff have questions on matters discussed in this report, please contact Randolph Hite at (202) 512-3439 or Keith Rhodes at (202) 512-6412. We can also be reached by E-mail at hiter@gao.gov and rhodesk@gao.gov, respectively. A GAO contact and key contributors to this report are listed in appendix III.

Randolph C. Hite
Director, Information Technology Architecture
and Systems Issues

Keith A. Rhodes
Chief Technologist, Applied Research and
Methods

Briefing Slides from April 19, 2002, Briefing to Staffs of Senators Helms and Warner

Information Technology: DOD Needs to Improve Process for Ensuring Interoperability of Telecommunications Switches

Briefing for the Staffs of
The Honorable Jesse Helms
and
The Honorable John Warner
United States Senate

April 19, 2002

1

Briefing Outline

- Introduction
- Objectives
- Scope and Methodology
- Background
- Results in Brief
- Results
  - Certification and Authorization Process Is Not Well-Defined
  - Process Has Been Inconsistently Applied, But Contracting Laws and Regulations Were Not Violated
  - Process Application Is Causing Vendors to Reevaluate Decision to Compete
- Conclusions
- Recommendations
- Agency Comments

2

Introduction

DOD policy requires systems to be interoperable. Interoperability can be viewed as the ability of systems to work together effectively and efficiently so that the right information gets to the right people at the right time.

Within DOD, the inability of systems to effectively and efficiently share information can have severe consequences. As we previously reported:

- A lack of basic interoperability led to problems in 1991 during the Persian Gulf war [1].
- Interoperability problems also arose in 1999 in Kosovo, which limited DOD's ability to rapidly identify and strike time-critical targets [2].

Accordingly, DOD's policy is that its communications systems, including telecommunications (telecom) switches, must be certified as interoperable [3].

[1] *Joint Military Operations: Weaknesses in DOD's Process for Certifying C4I Systems' Interoperability,* GAO/NSIAD-98-73 (Washington, D.C.: March 13, 1998).

[2] *Joint Warfighting: Attacking Time-Critical Targets,* GAO-02-204R (Washington, D.C.: November 30, 2001).

[3] Telecom switches are hardware and software designed to send and receive voice, data, and video signals across a network. For this briefing, the term "switch" refers to hardware and/or software installations for new switches or upgrades to existing switches.

3

Objectives

As agreed with the offices of Senators Helms and Warner, our objectives were to determine

- DOD's process for certifying and authorizing the interoperability of telecom switches,
- how the process is being applied, including whether contracting laws and regulations have been violated, and
- how the process affects vendor competition.

4

Scope and Methodology

To accomplish our objectives—

- We reviewed policy and procedures governing systems interoperability to obtain an understanding of the department's certification and authorization process for telecom switches (see appendix I for the policy and a list of the procedures).
- We assessed DOD's application of the process to five switch vendors' products to determine whether certification testing procedures were being followed and the requirements were being met.
  - We selected vendors whose products had been or currently were being tested for interoperability certification, and one vendor who had elected not to participate in the certification process. These vendors were
    - AG Commercial Systems,
    - Avaya,
    - Lucent Technologies,
    - Nortel Networks, and
    - Siemens.

5

Scope and Methodology (cont.)

- In assessing DOD's application of the process, we
  - obtained and reviewed test plans and results, request for and denial of a waiver, requests for and approvals of interim authorities to operate, certification letters, and supporting documentation when instances of noncompliance and/or deviations from the policy or process were identified; and
  - analyzed three awarded contracts and associated delivery orders.
    - Selected contracts awarded by the Army, Navy, and Air Force because, according to a key official responsible for enforcing the process, the military departments are the dominant purchasers of telecom switches.

6

Scope and Methodology (cont.)

- Selected delivery orders awarded for the European component of DOD's telecom switch modernization project. Specifically, we reviewed the following contracts and delivery orders:
  - Army's Digital Switched Systems Modernization Program contract and the Defense Information Systems Network–Europe (DISN-E) delivery order,
  - Air Force's Worldwide Integrated Digital Telecom Systems contract and the Spangdahlem (Germany) Switch Relocation and Upgrade delivery order, and
  - Navy's Voice, Video, and Data contract and the Replacement of Navy Defense Switching Network Telephone Switches (Italy) delivery order.

7

Scope and Methodology (cont.)

- Selected the Army's DISN-E delivery order for more detailed evaluation because**,** according to Army officials, it was the first delivery order that included the department's interoperability certification requirement. Specifically,
  - Reviewed the statement of requirements, which defined the requirements to be met by vendors competing for the award of this delivery order, including those related to interoperability.
  - Reviewed the results of Army's evaluation of the various vendors' proposals, including the technical solutions and price proposals.
    - Reviewed the winning vendor's technical proposal, which addressed its product's ability to meet DOD's requirements.

8

Scope and Methodology (cont.)

- Interviewed source selection and contract management officials responsible for evaluating the proposals and selecting the winning vendor to discuss
  - how the evaluation was conducted, and
  - whether the selected vendor met the interoperability requirements within the timeframe outlined in the statement of requirements.

9

Scope and Methodology (cont.)

To augment our document reviews and analyses, we interviewed officials from various DOD organizations, including

- the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (C3I)/Chief Information Officer,
- the director, Command, Control, Communications, and Computers Systems Directorate, Office of the Joint Chiefs of Staff,
- the Defense Information Systems Agency (DISA), including the Joint Interoperability Test Command and the Defense Switched Network Program Office,
- Army's Office of the Chief Information Officer,
- Army's Communications-Electronics Command Systems Management Center,
- Army's 5th Signal Command in Europe,

10

Scope and Methodology (cont.)

- Navy's Space, Information Warfare, Command and Control Directorate within its Office of the Chief of Naval Operations, and
- Air Force's single manager for telecommunications at the Ogden Air Logistics Center, Space and C3I Directorate.

We also interviewed representatives of the five telecom switch vendors to obtain their perspectives on DOD's certification and authorization process, DOD's application of the process, and the effect on their plans to compete for future business.

We did not independently validate the cost information we obtained during this review.

11

GAO
Accountability * Integrity * Reliability

Scope and Methodology (cont.)

As agreed with the requesters' offices, we did not review contracts and delivery orders for switches for intelligence systems or switches that are installed in tactical operations centers [4] or on board ships.

We conducted our work at DOD headquarters offices in Washington, D.C.; DISA's Joint Interoperability Test Command in Fort Huachuca, AZ; and Army's Communications and Electronics Command Systems Management Center in Fort Monmouth, NJ. The work was performed from August 2001 through April 2002 in accordance with generally accepted government auditing standards.

[4] Tactical operations centers are fixed and relocatable command posts where commanders and their staffs prepare, monitor, and alter the execution of battle plans.

12

Background

In November 1992, DOD issued a policy requiring systems, including telecom switches, to be tested and certified before approval is granted for installation in operational environments.

- In 1992 and 1995, DOD issued procedural instructions that were intended to document the process to be followed to achieve the policy's objective, and in 2000, it established the prioritization of systems to be tested and certified [5].

[5] For example, systems to be used to communicate nuclear warnings were to receive the highest priority. Those being acquired by individual defense agencies, but not used for this purpose, were to receive the lowest priority, because according to DOD, they are less critical to the department's primary mission.

13

Background (cont.)

In May 2000, almost 8 years after the original policy, the department began to enforce the policy for telecom switches.

- At that time, DOD began requiring that vendors' telecom switches be tested against and be certified as meeting interoperability requirements before being installed and connected to its network.

In fiscal year 2001, the military services reported that they spent approximately $90.8 million to acquire new telecom switches and upgrades to existing switches. In fiscal year 2002, the military services plan to spend about $78.6 million.

14

GAO
Accountability * Integrity * Reliability

Background (cont.)

Telecom Switch Requirements

DOD telecom switches are commercial products that are modified as necessary by the switch vendor to incorporate military-unique features.

- Military-unique features are requirements or capabilities that are not satisfied by a commercial product, but that DOD needs to accomplish a mission. Multilevel precedence and preemption is an example of such a feature [6].
- The military-unique features are documented in the department's *Generic Switching Center Requirements*. The latest version of these requirements is dated March 1997.

[6] This feature provides specific users with the capability to interrupt ongoing phone calls during emergency or crisis situations.

15

Background (cont.)

Defense Switched Network

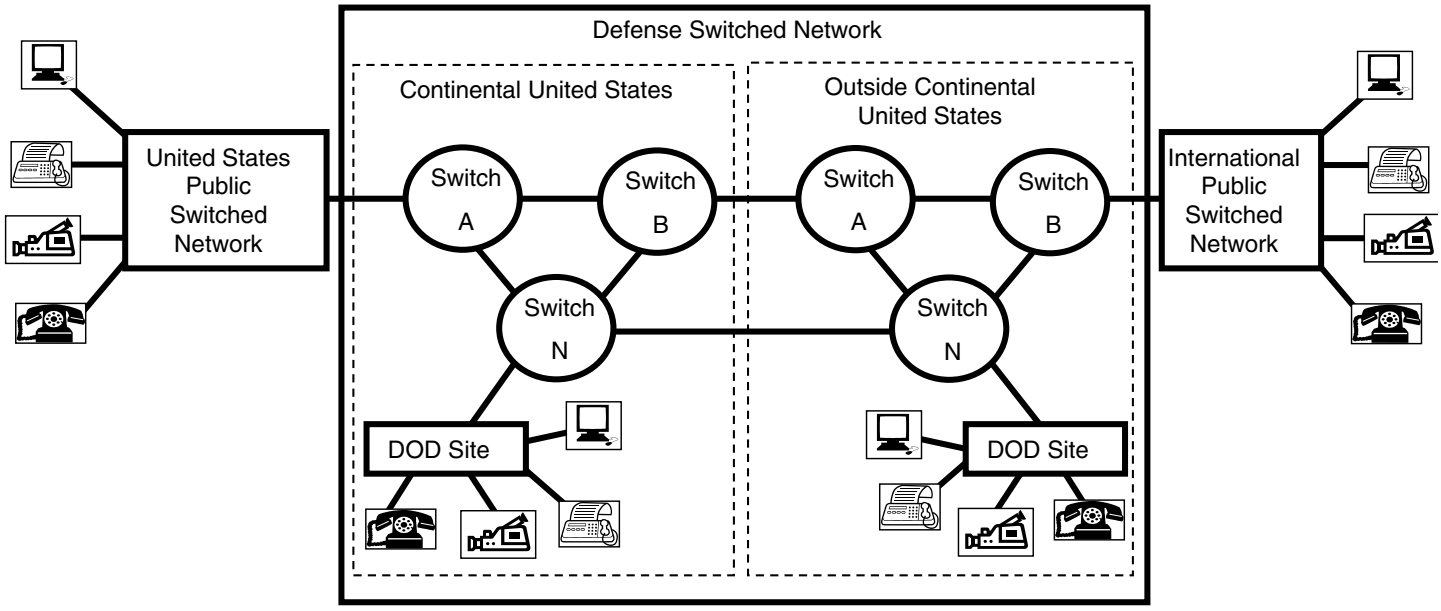
The Defense Switched Network provides telephone, data, and video-teleconferencing services for U.S. military bases and other DOD locations throughout the world. The network is under the operational direction and management control of DISA. The network is designated as a primary communication system during peacetime, periods of crisis, and the pre-attack, nonnuclear, and post-attack phases of war.

16

GAO
Accountability * Integrity * Reliability

Background (cont.)

Figure 1: Simplified Diagram of the Defense Switched Network



Source: GAO analysis of DOD material.

17

Background (cont.)

Prior Review of Interoperability Certification Process

In March 1998, we reported that the department did not have an effective process for certifying existing, newly developed, and modified systems for interoperability, resulting in noncertified systems. We also reported that the department did not know how many systems required certification [7]. We concluded that noncompliance with this requirement stemmed from weaknesses in the certification process itself and that continued noncompliance could jeopardize lives, equipment, and the success of joint military operations.

[7] GAO/NSIAD-98-73.

18

Background (cont.)

We recommended, among other things, that the department

- enforce its requirement that systems be tested and certified for interoperability before production and fielding unless official waivers are granted;
- develop a process for prioritizing systems for testing and certification; and
- develop a formal process for addressing interoperability problems observed during testing, and inform organizations that systems must be tested for interoperability.

DOD generally concurred with our recommendations and has taken steps to improve its interoperability certification process. Specifically, DOD has

- updated its policy and guidance to address enforcement weaknesses (e.g., established policies and procedures for validating systems' interoperability certification),
- developed criteria for prioritizing systems for testing and certification, and
- established some processes for addressing interoperability issues and monitoring waivers.

19

Results in Brief

Objective 1: DOD does not have a well-defined process, including clear requirements, for certifying and authorizing switches.

- DOD's telecom switch certification and authorization process is not fully documented, current, or complete. Additionally, the process lacks an effective enforcement mechanism.
- DOD officials attributed these weaknesses to the immaturity of the process.
- Without a well-defined process, DOD increases the risk that the certification and authorization of switches will not be done consistently and that its certification policy will not be met.

20

Results in Brief (cont.)

Objective 2: DOD has not applied its telecom switch certification and authorization process consistently across vendors, which in some cases violated policy. However, based on the scope of our work, we did not find that the department has violated contracting laws and regulations.

- The Army required one vendor to remove its uncertified switch from one location. At the same time, it allowed another vendor to install its uncertified switch at two locations, which violated the department's interoperability certification policy.
- Three of the five vendors we surveyed stated that DOD is not applying its process consistently.
- DOD officials agreed, attributing the inconsistency to the immaturity of the process.
- Based on the scope of our work, we did not find that the department has violated contracting laws and regulations.

21

Results in Brief (cont.)

Objective 3: DOD's telecom switch certification and authorization process is causing some vendors to reevaluate the department as a strategic customer.

- One of the five vendors we surveyed stated that it has stopped doing business with DOD because of this process and its implementation.
- Another vendor stated that it is reconsidering its participation in the DOD market because of perceived inequities in the department's application of the process.
- According to a Joint Staff official responsible for enforcing the process, the department's implementation of this process will not negatively affect competition.

22

Results in Brief (cont.)

Recommendations

To assist DOD in achieving its goals of ensuring network interoperability and promoting competition among telecom switch vendors, we are recommending that the secretary of defense take specific near-term and longer term actions that are intended to strengthen the department's switch certification and authorization process.

In commenting on a draft of this briefing, DOD officials agreed with our findings and largely agreed with our conclusions and recommendations.

23

GAO
Accountability * Integrity * Reliability

Results
Objective 1: Process

DOD does not have a well-defined process, including clear interoperability requirements, for certifying and authorizing telecom switches.

Prudent management suggests that for a process to be effective and efficient, it should be (1) documented, (2) current, (3) complete, and (4) enforceable.

DOD's telecom switch certification and authorization process does not fully satisfy any of these four tenets, because according to department officials, the process is relatively new, having until recently been assigned a relatively low priority.

Until these four process weaknesses (discussed in detail on the following pages) are corrected, DOD increases the risk of inconsistently applying the process and of experiencing future interoperability problems.

24

GAO
Accountability * Integrity * Reliability

Results
Objective 1: Process (cont.)

Process Not Fully Documented

Process effectiveness and efficiency depend in part on whether the process is fully documented.

The department's process for certifying and authorizing telecom switches is not fully documented. Therefore, using available documentation, supplemented by interviews of the process stakeholders identified on page 27, we graphically documented the process (see pages 28 through 34). In documenting the process, we divided it into seven process areas, each consisting of multiple steps and decision points.

- Out of the seven process areas (schedule product, test, validate, authorize, appeal, install and connect, and request interim authority to operate), DOD had documented less than half the process steps for three of the areas: test, validate, and appeal.

25

Results
Objective 1: Process (cont.)

- In the test area, for example, DOD had documented only 1 of the 10 major steps that we defined in depicting the process.
- Further, with respect to appealing test results, while DOD instructions identify the organizations that hear appeals when issues arise during testing, they do not document the procedures to be followed nor the expected outcome of successful appeals (that is, whether switches receive certifications or interim authorities to operate). Moreover, one of the five vendors was unaware that an appeals process existed.

DOD officials agreed that the process was not fully documented and stated that our representation was an accurate depiction.

26

GAO
Accountability * Integrity * Reliability

Results
Objective 1: Process (cont.)

Table 1: Process Stakeholders' Roles and Responsibilities

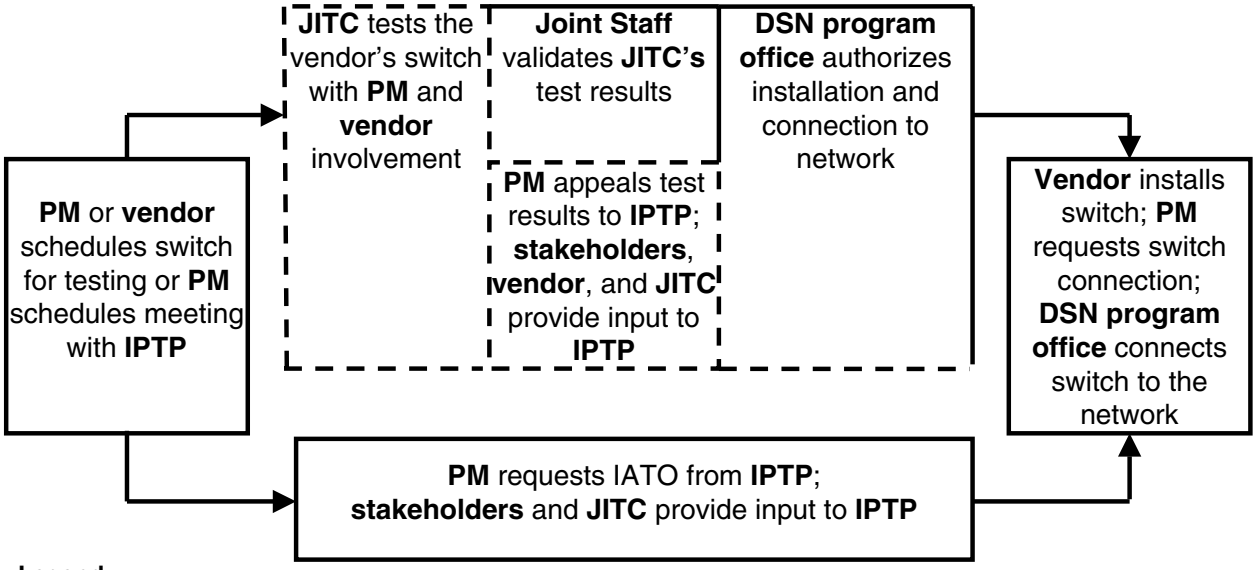
Organization	Responsibility/function
Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (C3I)/Chief Information Officer	Maintains the interoperability policy and provides guidance and oversight. Implements the interoperability policy and procedures if designated as the program's decision authority.
DISA's Joint Interoperability Test Command (JITC)	Tests and certifies switches for interoperability.
DISA's Defense Switched Network (DSN) program office	Authorizes the installation and connection of switches to the DSN.
Chairman of the Joint Chiefs of Staff	Establishes operational procedures for certifying and authorizing interoperability.
Joint Staff, Command, Control, Communications, and Computers Systems Directorate	Enforces the interoperability policy and procedures.
Interoperability Policy and Test Panel (IPTP)	Resolves interoperability policy and testing issues and hears appeals.
Military Communications-Electronics Board	Resolves issues if the IPTP is unable to do so.
Heads of DOD component organizations	Plan, program, budget, and provide resources for interoperability testing programs, and implement the interoperability policy and procedures.
Program Manager (PM)	Coordinates testing activities, appeals test results, requests interim authorities to operate, and requests connection of switch to the network. Implements the interoperability policy and procedures if designated as the program's decision authority.

27

GAO
Accountability * Integrity * Reliability

Results
Objective 1: Process (cont.)

Certification and Authorization Process Overview



Legend:

IATO: Interim Authority to Operate

Note: Dashed boxes indicate areas of the process that DOD has not documented. Information related to these process areas was obtained through interviews with DOD process stakeholders and review of documentation on specific switch certification and authorization actions produced as a result of the process.

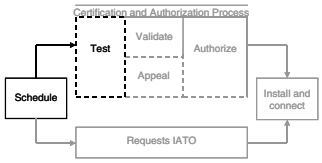
Source: GAO analysis of DOD-supplied evidence.

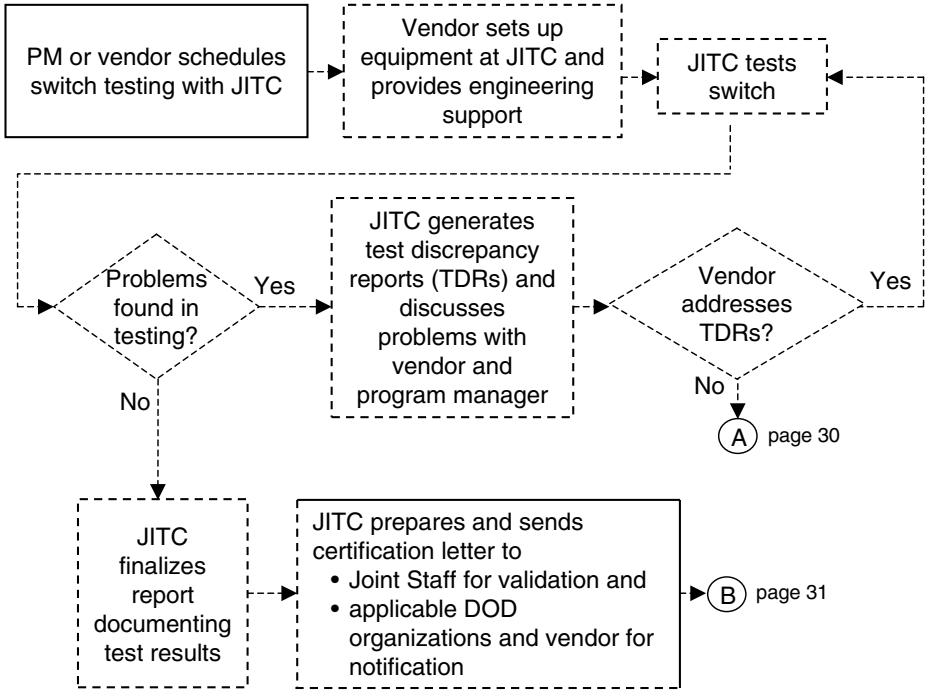
28

GAO
Accountability * Integrity * Reliability

Results

Objective 1: Process (cont.)





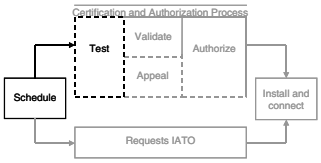
Source: GAO analysis of DOD-supplied evidence.

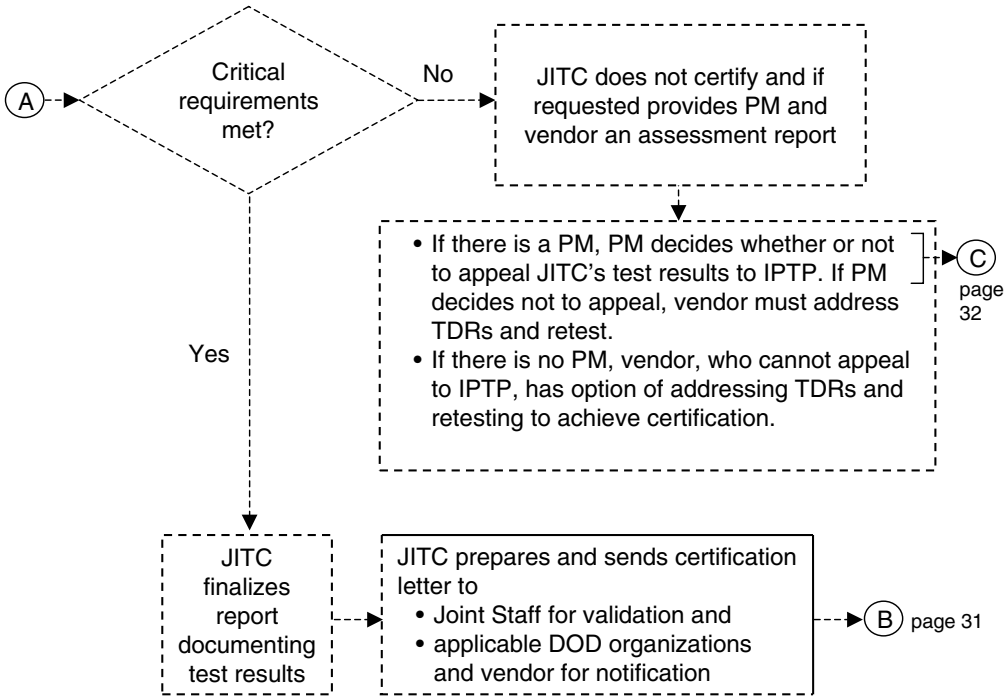
29

GAO
Accountability * Integrity * Reliability

Results

Objective 1: Process (cont.)

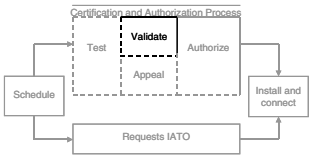


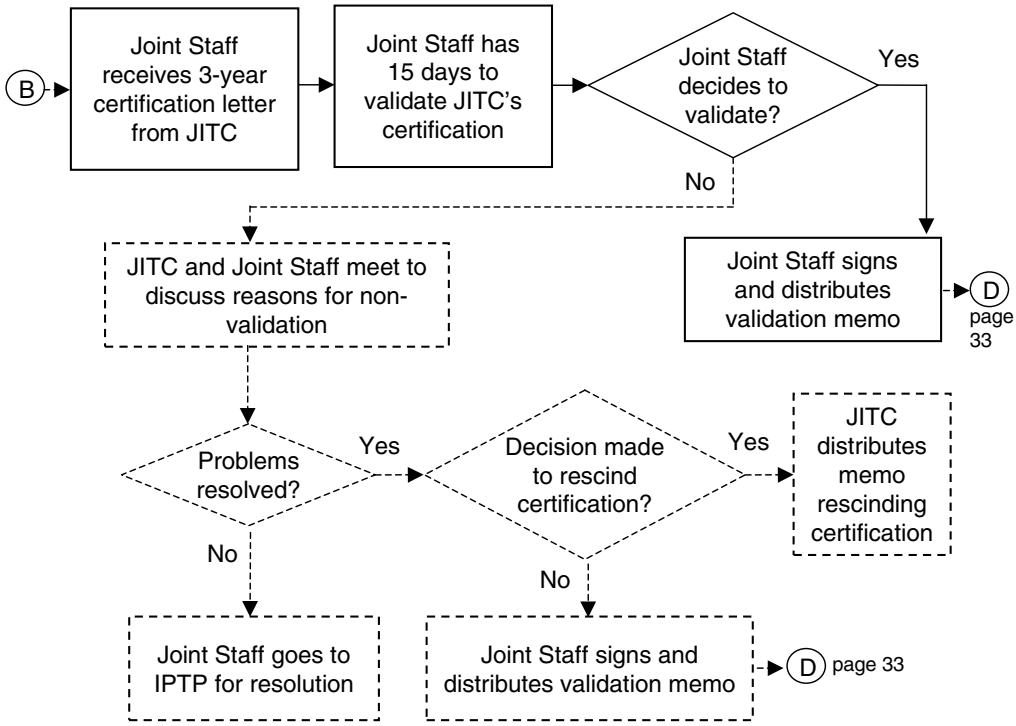


Source: GAO analysis of DOD-supplied evidence.

GAO
Accountability * Integrity * Reliability

Results
Objective 1: Process (cont.)



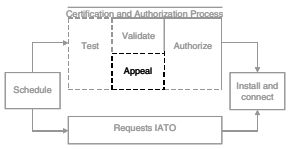


Source: GAO analysis of DOD-supplied evidence.

31

GAO
Accountability * Integrity * Reliability

Results
Objective 1: Process (cont.)



C

PM decides to appeal test results to IPTP

PM presents its case and test results to IPTP; stakeholders, vendor, and JITC provide input

IPTP reviews case and determines potential operational impact of installing switch

IPTP determines that outstanding TDRs present a significant risk?

Yes

IPTP informs PM and JITC of its decision. JITC does not issue a certification letter.
PM may
- accept IPTP's decision and agree to resolve TDRs or
- appeal to Military Communications-Electronics Board.

No

IPTP has option of issuing an IATO or a memo to JITC asking it to issue a certification letter.
- According to a JITC official, JITC would require a written document from IPTP detailing agreements reached before issuing a certification letter.

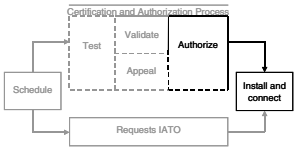
E
page 33

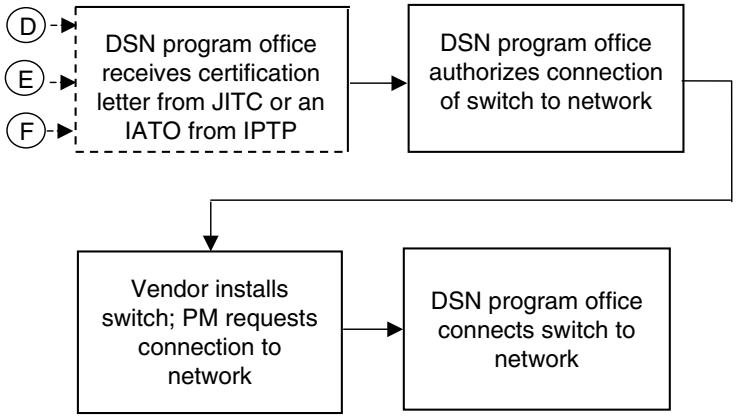
Source: GAO analysis of DOD-supplied evidence.

32

GAO
Accountability * Integrity * Reliability

Results
Objective 1: Process (cont.)



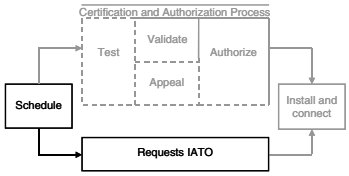


Source: GAO analysis of DOD-supplied evidence.

33

GAO
Accountability * Integrity * Reliability

Results
Objective 1: Process (cont.)



PM schedules meeting with IPTP by submitting an IATO application for a specific vendor's switch at a specific location

PM meets with IPTP to discuss the request; stakeholders and JITC provide input

IPTP approves IATO?

No

IPTP does not issue an IATO. PM can appeal to Military Communications-Electronics Board by submitting the IATO application

Yes

IPTP issues IATO for a period not to exceed 1 year

F page 33

Note:

An IATO may be granted if there is an immediate need for a switch to be installed, and the operational risk to the network of installing this uncertified switch is minimal.

The vendor's switch is to proceed through the certification process during the time the IATO is in effect; 90-days before IATO expiration, JITC notifies the PM, who can request a new IATO if the switch will not be certified before the IATO expires.

Source: GAO analysis of DOD-supplied evidence.

34

GAO
Accountability * Integrity * Reliability

Results
Objective 1: Process (cont.)

Switch Requirements Are Outdated

For a process to be implemented effectively and efficiently, it should be current.

According to DOD policy, switch requirements that define the military-unique features are to be revised every 2 years. However, this has not occurred.

- The latest version of the requirements is dated March 1997.
- DOD has posted a draft of its updated requirements on its website and is soliciting vendors' comments. DOD plans to issue the revised requirements in final form in September 2002.

35

Results
Objective 1: Process (cont.)

Switch Requirements Are Not Complete

For a process to be implemented effectively and efficiently, it should be complete.

DOD's switch requirements are incomplete in that they either have not been defined with a sufficient level of detail or are not defined at all. For example,

- Our review of the requirements showed that while there was sufficient detail for testing major switches, such as multifunctional switches [8], the requirements did not address other types, such as remote switching units. In addition, the requirements currently do not address new technology, such as voice over Internet protocol (VOIP) [9], which is currently being installed throughout DOD's services and agencies.

[8] A multifunction switch provides both local and long-distance services.

[9] VOIP is an efficient, cost-effective way of transporting voice traffic across Internet networks.

36

GAO
Accountability * Integrity * Reliability

Results
Objective 1: Process (cont.)

- Vendors stated that the requirements for the military-unique features are not complete in that they do not always have the level of detail required for designing and developing military-unique features, and that they do not exist in other cases, such as for remote switching units and VOIP technology [10].
- JITC officials agreed that there are test scenarios for which the requirements do not provide enough detail to enable JITC to design and execute related test plans; they also confirmed that requirements do not exist for certain switch types (e.g., remote switching units) and advances in technology (e.g., VOIP).
    - Further, JITC officials reported that current revisions to these requirements will not address all the vendors' concerns.
- Army officials reported that the certification of one vendor's switch was held up for months because there were no defined requirements for that switch type.

[10] Remote switching units are controlled by a host switch, but are located separately from the host.

37

GAO
Accountability * Integrity * Reliability

Results
Objective 1: Process (cont.)

Process Does Not Provide an Effective Means for Enforcing

Process effectiveness and efficiency depend on whether enforcement mechanisms are in place and functioning as intended.

The Joint Staff [11] is responsible for enforcing the process; however, these officials told us that their ability to enforce is limited to making all process stakeholders aware of the interoperability certification requirement and directing the DSN Program Office to connect only certified switches to the network.

The Director of DISA stated that the current enforcement process can be strengthened.

[11] The Joint Staff, Command, Control, Communications, and Computers Systems Directorate.

38

Results
Objective 1: Process (cont.)

According to officials in the DSN program office, it is difficult to enforce the interoperability certification policy, because the DSN program office does not monitor all switch installations or upgrade activities, and is not always informed by the military services or defense agencies of installations of new switches or upgrades to existing switches to the network. The DSN program office knows with certainty only about the switch installations or upgrades that require it to make modifications to the network.

- Currently, DISA is surveying the military services and agencies to compile an inventory of existing switches connected to the network to obtain a baseline.

39

GAO
Accountability * Integrity * Reliability

Results
Objective 1: Process (cont.)

Consequences of Process Not Being Well-Defined and Enforceable

Because the process is not well-defined, it is also not well understood by the DOD participants and vendors. For example,

- The term "certification," which is not specifically defined within the policy and procedures, has been interpreted differently by different stakeholders. One vendor told us it means *global* certification (i.e., the switch complies with all applicable requirements and can be installed at any U.S. base worldwide). However, DOD officials told us that there can be degrees of certification (e.g., *limited* certification, in which case the switch cannot be globally installed, but can be installed within certain operational environments).
- The process is set up so that only a department representative can appeal test results. The process also allows a vendor to submit its product for testing without a DOD sponsor. Thus, in this case the process would not permit a vendor to appeal the test results, because the vendor would lack a DOD representative to present the appeal. Army officials and vendors, who were aware of the appeals process, did not know this.

40

Results
Objective 1: Process (cont.)

- The Joint Staff recently issued a memorandum that is being interpreted by Army and vendors as a certification letter that recommends global use of a specific switch. However, under the process, only JITC can certify a switch. In this instance, JITC has not issued a certification letter recommending global use of this switch. Moreover, DISA has not decided whether it will authorize connection of the switch based on this memorandum or if it will need JITC to issue a certification letter.
  - According to the Joint Staff official who signed the memorandum, it was issued in response to an inquiry by a DISA official regarding the operational risks of installing a specific switch that still had unresolved deficiencies. The memorandum was not intended to globally certify the switch, since only JITC can certify switches as having met the interoperability requirements.

41

Results
Objective 1: Process (cont.)

Because there is no effective enforcement mechanism, DOD has increased its risk of inconsistently applying the process and of experiencing future interoperability problems.

To fill the gaps in its process, DOD is currently reviewing the procedures governing the process.

- DOD has not established a time frame for when the procedures supporting the policy will be revised and issued.

42

GAO
Accountability * Integrity * Reliability

Results
Objective 2: Application of Process

DOD has not applied its interoperability certification and authorization process for switches consistently across all vendors, which in some cases violated policy. However, based on the scope of our work, we did not find that it has violated applicable contracting laws and regulations.

DOD has not consistently applied its telecom switch certification and authorization process, at times treating different vendors differently and violating its interoperability certification policy.

- For example, the Army required one vendor to remove its uncertified switch from one location, while at the same time allowing another vendor to install its uncertified switch at two locations.
- Further, Army allowed another vendor to install its uncertified switch, and this vendor has since stated that it has no plans to test its switch with JITC.

43

Results
Objective 2: Application of Process (cont.)

Also, three of the five vendors we interviewed stated that the process is not being applied consistently.

- Two vendors stated that DOD has allowed competitors to install uncertified products while requiring them to have switches certified before installation.

DOD acknowledged inconsistencies in the application of the process and stated that these inconsistencies were due to the process being new and evolving.

Among other things, this inconsistency has resulted in uncertified switches being connected to DOD's network, which increases the risk of potential service disruptions.

Despite the inconsistency in the process' application, the switch contracts and delivery orders that we reviewed did not show that DOD has violated contracting laws and regulations in implementing this requirement.

44

Results
Objective 2: Application of Process (cont.)

Inconsistent Application: Compliance with Interoperability Policy

The Army allowed one vendor to install an uncertified version of a switch on DSN (the switch was at the time undergoing certification testing). When DISA verbally notified the Army that there were testing concerns, the Army required the vendor to remove this version of the switch pending certification and to install the prior version of the switch. Once the new version was certified, the Army authorized the vendor to install it.

The Army has also installed another vendor's switches that were either certified or had been issued IATOs at various locations.

The Navy and Air Force installed only certified switches for the locations we reviewed.

45

GAO
Accountability * Integrity * Reliability

Results
Objective 2: Application of Process (cont.)

Inconsistent Application: Noncompliance with Interoperability Policy

The Army allowed one vendor to install an uncertified upgrade to a switch. While this version of the switch had been installed before the Army began enforcing the interoperability certification requirement, the upgrade was subject to the requirement, and it had not been granted an IATO. After installation, the vendor elected not to seek certification of its switch because of the expense involved.

- According to Army officials,the upgraded switch was not removed because the upgraded version had been installed at other locations before DOD began enforcing its certification requirement, and it was performing satisfactorily.
- DISA officials agreed that it was appropriate to waive the interoperability certification requirements for these installations.

The Army also installed another vendor's uncertified switch without an IATO at two other locations. The switch was installed before JITC completed certification testing. After installation, an IATO was requested and granted for these two locations.

46

Results
Objective 2: Application of Process (cont.)

Inconsistent Application: Noncompliance with Interoperability Policy (cont.)

The Army also allowed another vendor to install an uncertified switch without an IATO at another location. While an IATO had been previously granted, the IATO was for an earlier version of the switch, not the actual version installed. The Army later requested and received an IATO for the actual version of the switch that was installed.

The Army installed still another vendor's switch at three locations that had neither been certified nor granted an IATO.

- DISA officials agreed with the Army that it was appropriate to waive the interoperability certification requirements for these installations, since the switches were acquired via fiscal year 2000 delivery orders and already installed at other locations within the DSN.

47

Results
Objective 2: Application of Process (cont.)

Inconsistent Application: Noncompliance with Interoperability Policy (cont.)

The Joint Staff has issued a memorandum that is being interpreted by Army and vendors as validating global certification of one vendor's switch with certain restrictions [12]. However, according to DOD's certification and authorization process, JITC must certify the switch before the Joint Staff can validate the certification. In this instance, JITC has not certified the switch for global use because the switch has not met the requirements for global certification.

- According to Joint Staff officials, the memorandum was not intended to validate global certification for this switch.
- Three vendors stated that this action by the Joint Staff undermines the integrity of DOD's interoperability certification process.

[12] Memorandum for Defense Information Systems Agency, Attn: Congressional Affairs, *Elektronisches Waehl System Digital (EWSD) Release 18 Test Issues,* January 2, 2002; signed by General Croom.

48

GAO
Accountability * Integrity * Reliability

Results
Objective 2: Application of Process (cont.)

Inconsistent Application: Noncompliance with Interoperability Policy (cont.)

According to DOD officials, some services and agencies (e.g., Navy, DISA) are installing voice over Internet protocol (VOIP) switches at locations (e.g., the Washington Navy Yard and DISA headquarters) without meeting requirements for interoperability testing and certification.

- The reason for not complying with the policy is that requirements for implementing and testing requirements for VOIP switches have not been defined.
- One vendor is currently testing its VOIP switch and assisting JITC in establishing the requirements.
- At the same time that one vendor is testing its VOIP switch, another vendor is being allowed to install VOIP switches without certification.

In instances where requirements do not exist, the process provides for requesting an IATO until such time as the requirements are defined and testing can begin. However, DOD officials acknowledged that until recently this had not been done and that in the above cases IATOs were not issued.

49

Results
Objective 2: Application of Process (cont.)

Joint Staff and DISA officials acknowledged that there have been inconsistencies in the application of the process and stated that these inconsistencies were due to the process being new and evolving.

50

Results
Objective 2: Application of Process (cont.)

Compliance with Contracting Laws and Regulations

Federal laws and regulations allow the government to take action other than termination when a vendor does not meet requirements. In such a case, the government is required to obtain consideration from the vendor. Such consideration might include reductions in payment to offset the reduction in the contractor's obligation.

On the basis of the switch contracts and delivery orders that we reviewed, the Navy and Air Force have consistently included interoperability as a contractual requirement. Specifically,

- The Navy and Air Force awarded delivery orders to one vendor whose switch was already certified and authorized.

Army included the requirement for interoperability certification as a contractual requirement and, based on the scope of our work, complied with contracting laws and regulations in implementing this requirement. Specifically,

51

GAO
Accountability * Integrity * Reliability

Results
Objective 2: Application of Process (cont.)

- The Army awarded a delivery order to a vendor whose product has not yet met the global certification requirement.
  - However, in this case, the Army received consideration from the vendor for failure to perform, as required under federal law.
    - The vendor's product did not pass the initial 30-day evaluation of its interoperability capabilities, as required. As consideration for this, the Army negotiated a new payment schedule that was advantageous to the government.
    - The vendor's product did not receive global certification within 270 days of the delivery order award as required. Again, the Army received consideration, including, among other things, extended warranties and free equipment and training.
  - According to the Army, this vendor's product was still the best value because of this consideration, and no other vendors' products were certified at that time.

52

Results
Objective 2: Application of Process (cont.)

When contracts are competed, federal laws and regulations generally require the government to provide vendors an equal opportunity to be awarded the contract, referred to as "full and open competition." However, laws and regulations are more flexible for the award of delivery orders under existing contracts. When delivery orders are competed, the government must provide vendors a "fair opportunity to be considered," which is a much less stringent standard. For example,

- When delivery orders are competed, contracting officers may exercise broad discretion, including
  - using streamlined procedures, such as oral presentations, and
  - not contacting or holding discussions with each awardee under the contract before selecting an awardee for the delivery order.

53

Results

Objective 2: Application of Process (cont.)

For delivery orders under the Digital Switched Systems Modernization Program contract including DISN-E, the Army defined specific procedures for the source selection process. These included specifying that

- vendor selection be determined using a “best value” approach that would consider, among other things, the technical solution being proposed by the vendors (hardware and software) and the cost to the government; and
- the department consider any special circumstances, such as urgency for requirements and/or funding constraints, that could prevent some requirements from being competed between multiple contractors.

54

Results
Objective 2: Application of Process (cont.)

Based on the scope of our work, the Army's implementation of the source selection process for the DISN-E delivery order did not violate federal laws and regulations. For example:

- Although the Army allowed the winning vendor to change its original proposed product late in the source selection process and did not conduct a further evaluation of the newly proposed product, this was not a violation of federal laws and regulations because (1) revisions of proposals are permitted in the negotiation process, (2) the Army was following streamlined procedures applicable to delivery orders, and (3) the Army found that the change in proposed product did not materially affect the vendor's technical proposal.

According to Army officials, the vendor's switch that was selected provided the "best value" among competing vendors' proposals.

55

Results
Objective 2: Application of Process (cont.)

In appendix II, we provide a timeline showing the sequence of the relevant events involved in DOD's establishment of its telecom switch certification and authorization process and the department's application of the process to the vendors' products included in our review, as described in the previous slides.

56

GAO
Accountability * Integrity * Reliability

Results
Objective 3: Competition

DOD's application of its interoperability certification and authorization process is influencing vendors' plans for competing.

The department's goals are to ensure that its interoperability requirements are met and to promote competition among telecom switch vendors in doing so.

Four of the five telecom switch vendors we interviewed supported DOD's goal of ensuring switch interoperability. However, questions are emerging relative to the second goal because vendors are reconsidering their plans for having DOD as a strategic customer.

- The one vendor that has not stated its support of DOD's goal has chosen not to participate for economic reasons (i.e., the costs associated with testing and certification exceed potential business opportunities with DOD).
- Another stated that it is re-evaluating its decision to participate in this process because of concerns about DOD's inconsistent application of the process.

57

GAO
Accountability * Integrity * Reliability

Results
Objective 3: Competition (cont.)

Questions are also surfacing within the department as to the impact of the process on competition. For example:

- An Army telecom program manager stated that he expected other vendors to cease doing business with the department because of the cost and problems associated with the certification and authorization process.

Positions within the department are mixed on the impact of DOD's interoperability goal on competition. For example,

- DISA's congressional liaison official stated that the department is not concerned that some vendors, especially 1 or 2, may elect not to compete as a result of the department's implementation of this process. This official noted that this could in fact strengthen competition by eliminating those vendors who are less willing to comply with the department's requirements.
- Army officials stated that the loss of any vendors would have a negative effect on competition.
- A Joint Staff official responsible for enforcing the process stated that the department's implementation of this process will not negatively affect competition.

58

Conclusions

DOD's process for ensuring that telecom switches are interoperable before being installed for operational use on its network can be improved. As currently defined and implemented, this process permits uncertified switches to be installed, thus risking network performance shortfalls that could impair DOD's ability to meet mission objectives. Better definition and enforcement of the process would reduce the risk of network interoperability problems and potentially increase competition.

The weaknesses in the process can be traced to several factors, including the following:

- the process is only partially documented, and switch certification requirements are outdated and incomplete, and
- the process does not provide for effective enforcement.

59

Conclusions (cont.)

Given these limitations, DOD has not consistently applied the process to telecom switch vendors. While some of this inconsistent application was not outside the bounds of the process as it is defined, some of it was, such as when DOD required one vendor to remove its uncertified switch, while at the same time allowing another vendor to install its uncertified switch. Such actions were, in our view, the product of bad decisionmaking by the service that implemented the process. While these actions violated DOD's policy, they did not however, based on the scope of our work, constitute any violations of contracting laws and regulations.

60

Recommendations

To ensure network interoperability and address the potential impact on competition for telecom switch vendors, we recommend that the secretary of defense advance the state of maturity of DOD's telecom switch certification and authorization process by directing the chairman of the Joint Chiefs of Staff, as the DOD authority responsible for the process, to take the following near-term and long-term actions to improve the process.

In the near term,

- use the process flowcharts provided in this briefing to assist in fully documenting the existing certification and authorization process, and
- make this fully documented process available to DOD and vendor process stakeholders within 60 days.

61

Recommendations (cont.)

In the longer term, revise the existing process including switch requirements to ensure that it is complete, current, transparent to stakeholders, and enforceable by the Joint Staff, and issue a revised process to all stakeholders within 180 days. In doing so, the chairman should

- work jointly with the assistant secretary of defense for C3I since this organization is responsible for the interoperability policy and for providing guidance and oversight,
- solicit DOD and vendor input on needed process changes, and
- seek DOD and vendor comments on a draft of the revised process before it is issued in final form.

62

Recommendations (cont.)

We also recommend that the secretary direct the director of DISA, as the DOD authority responsible for certifying the interoperability of switches, to complete its ongoing inventory of installed DSN switches. Using this inventory, we further recommend that the secretary direct the assistant secretary of defense for C3I, in collaboration with the chairman, to assess the level of DSN interoperability risk associated with having uncertified switches on the network and to develop and implement a risk mitigation strategy to address any risks identified.

63

Agency Comments

We provided a draft of this briefing to DOD officials representing the Office of the Assistant Secretary of Defense for C3I (ASD/C3I), the Joint Staff, the Defense Information Systems Agency (including the Joint Interoperability Test Command and the Defense Switched Network Program Office), and Army's Communications-Electronics Command Systems Management Center. Among these officials were ASD/C3I's chief of information interoperability and Army's Project Manager for its Defense Communications and Army Switched Systems.

In commenting on the draft, these officials agreed with our findings and largely agreed with our conclusions and recommendations.

64

Agency Comments (cont.)

The officials did however provide clarifying information and suggested refinements to one of our conclusions on the effect of process weaknesses, which we have incorporated as appropriate. They also stated that our draft recommendation regarding the need to establish a policy governing situations when switch requirements have not been defined was not needed because the process already addresses this. We agreed with their position and thus are no longer making the recommendation.

65

GAO
Accountability * Integrity * Reliability

Appendix I:
DOD Policy and Procedures

Department of Defense Directive 4630.5, *Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence Systems* (November 12, 1992; revised January 11, 2002), states that all IT systems are to be designed for joint use, with interoperability requirements defined in the initial stages of IT system development. This directive also outlines responsibilities of DOD components within the interoperability process, including the chairman of the Joint Chiefs of Staff's responsibility for ensuring compliance with interoperability certification requirements.

Department of Defense Instruction 4630.8, *Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence Systems* (November 18, 1992; currently being revised), further details DOD components' responsibilities for the interoperability certification process.

66

GAO
Accountability * Integrity * Reliability

Appendix I:
DOD Policy and Procedures (cont.)

Chairman of the Joint Chief of Staff Instruction 6212.01, *Interoperability and Supportability of National Security Systems and Information Technology Systems* (June 30, 1995; revised May 8, 2000), establishes procedures for the certification and validation of IT systems. It also establishes the DOD chief information officer as the focal point for ensuring the interoperability of systems throughout the department.

Chairman of the Joint Chief of Staff Instruction 6215.01, *Policy for the Department of Defense Voice Networks* (February 1, 1995; revised September 23, 2001), states that the Defense Switched Network is to be designed with the capability to permit interconnection and interoperability.

67

GAO
Accountability * Integrity * Reliability

Appendix I:
DOD Policy and Procedures (cont.)

Military Communications-Electronic Board reference guide, *Organization, Mission and Functions* (January 1, 2002), lists the organizations, mission, and functional aspects of the panels and working groups of the Military Communications-Electronic Board. This board acts as the senior resolution body in the certification process.

The *Interoperability Policy and Test Panel Charter* (June 6, 2001; reissued January 1, 2002, in the Military Communications-Electronic Board reference guide*, Organization, Mission and Functions*) outlines interim authority to operate procedures and describes the general functions of the panel, including identifying, coordinating, and resolving interoperability policy and testing issues.

68

GAO
Accountability * Integrity * Reliability

Appendix II
Timeline

			Vendors				
Year	**Congress**	**DOD**	**AGCS**	**Avaya**	**Lucent**	**Nortel**	**Siemens**
Pre-1997		**November 12, 1992** DOD issues directive requiring all information technology systems to be interoperable **November 18, 1992** DOD issues instruction detailing responsibilities for interoperability certification process **February 1, 1995** Chairman of Joint Chiefs of Staff (CJCS) issues instruction requiring similar components of Defense Switched Network (DSN) to be interoperable **June 30, 1995** CJCS issues instruction on interoperability process **November 6, 1996** DISA issues request for information (RFI) for the Defense Information Systems Network-Europe (DISN-E)					
1997		**January 10** Initial RFI response deadline **February 7** Extended RFI response deadline			**February 7** Lucent responds to RFI	**February 7** Nortel responds to RFI	**February 7** Siemens responds to RFI

GAO
Accountability * Integrity * Reliability

Appendix II
Timeline (cont.)

			Vendors				
Year	Congress	DOD	AGCS	Avaya	Lucent	Nortel	Siemens
1998		**September 11** Army issues statement of requirements (SOR) for DISN-E					
		December 2 Army decides to pay testing costs for DISN-E winning vendor					
1999		**January 6–7** Source selection panels hear oral presentations from vendors for DISN-E SOR			**January 4** Lucent submits proposal for DISN-E contract	**January 4** Nortel submits proposal for DISN-E contract	**January 4** Siemens submits proposal for DISN-E contract
		January 8 Source selection panels begin reviewing proposals for DISN-E SOR					
							February 12 Siemens switches product from European to American standards
		February 24 Source selection panels complete proposal reviews					
		March 4 Army awards contract to Siemens					**March 4** Siemens wins DISN-E award

GAO
Accountability * Integrity * Reliability

Appendix II
Timeline (cont.)

Year	Congress	DOD	Vendors				
			AGCS	Avaya	Lucent	Nortel	Siemens
1999 (cont.)		**April 7–22** Army conducts limited test and evaluation of Siemens' EWSD switch					
		April 26 Army issues show cause letter to Siemens, threatening contract cancellation					**April 22** Siemens receives "unsatisfactory" result on 30-day limited test and evaluation of switch
							May 5 Siemens responds to show cause letter, 2 days after deadline
							June 14–15 Siemens demonstrates required capability to Army's satisfaction
		June 21 Army rescinds show cause letter based on Siemens' demonstration of switch capability					

GAO
Accountability * Integrity * Reliability

Appendix II
Timeline (cont.)

Year	Congress	DOD	Vendors				
			AGCS	Avaya	Lucent	Nortel	Siemens
1999 (cont.)		**July 16** Army and DISA establish eight minimum requirements for Siemens' EWSD switch certification					
		July 27 Army agrees to contract considerations made in response to Siemens' test failure					**July 27** Siemens agrees to contract considerations after failing test
		September 9 Army awards delivery order to General Dynamics (a Nortel distributor) for switch upgrades in Korea and Japan					
							October 12 Siemens starts testing at JITC of EWSD switch, rel. 16
						October 20 Nortel starts testing MSL11 at JITC	
		December 8 Army & DISA direct JITC to stop testing of EWSD rel. 16 due to significant problems					**December 8** Siemens stops testing rel. 16 with JITC

GAO
Accountability * Integrity * Reliability

Appendix II
Timeline (cont.)

Year	Congress	DOD	Vendors				
			AGCS	Avaya	Lucent	Nortel	Siemens
1999 (cont.)							**December 17** Siemens fails to meet 270-day certification requirement as outlined in contract
2000		**March 27–29** Army and Siemens agree to "get well" plan as remedy for Siemens' failure to meet the 270-day certification requirement					**March 27–29** Army and Siemens agree to "get well" plan as remedy for Siemens' failures to meet the 270 – day certification requirement
		May 1 Joint Staff issues memo stating that upgrades to DSN must be interoperable					
		May 8 CJCS revises instruction further detailing interoperability process					
		June 21 Army agrees to contract considerations made in response to Siemens' failure to meet 270-day deadline					**June 21** Siemens agrees to contract considerations in response to failure to meet 270-day deadline

73

GAO
Accountability * Integrity * Reliability

Appendix II
Timeline (cont.)

			Vendors				
Year	Congress	DOD	AGCS	Avaya	Lucent	Nortel	Siemens
2000 (cont.)		**July** DISA orally authorizes Army to install uncertified EWSD switches at 2 sites				**July 11** Nortel installs uncertified MSL12 at Qatar	
		July 21 Army directs Nortel to remove uncertified MSL12 switch at Qatar					
		July 28 Army sends letter to General Dynamics halting installation activities for Korea and Japan				**July 31** Nortel starts testing MSL12 at JITC	
		August 2 Navy awards delivery order to General Dynamics to upgrade switches in Italy				**August 4** Nortel receives certification of MSL11	
						August 9 Nortel deinstalls uncertified switch at Qatar	

74

GAO
Accountability * Integrity * Reliability

Appendix II
Timeline (cont.)

			Vendors				
Year	Congress	DOD	AGCS	Avaya	Lucent	Nortel	Siemens
2000 (cont.)							**August 18** Siemens installs uncertified EWSD, rel. 16, at Funari, Germany
				August 25 Avaya installs uncertified switch at Pine Bluff Arsenal			
		August 30 Army authorizes AGCS to install uncertified switch upgrades at Sierra Army Depot and Fort Gordon					
		September 20 Air Force issues upgrade order for DSN switch in Germany to Nortel, which was only certified switch available to DOD					**September 22** Siemens installs uncertified EWSD, rel. 16, at Coleman Barracks, Germany
		September 25 Military Communications-Electronics Board requests that the Joint Staff review DOD's need for military-unique requirements					
			September 30 AGCS installs uncertified upgrade at Sierra Army Depot				

75

GAO
Accountability * Integrity * Reliability

Appendix II
Timeline (cont.)

			Vendors				
Year	Congress	DOD	AGCS	Avaya	Lucent	Nortel	Siemens
2000 (cont.)	**October 6** Senator John Warner asks Secretary of Defense for information regarding uncertified hardware and software connected to DSN						
		October 20 DISA issues formal memo stating support of EWSD switch installation at Funari and Coleman Barracks. Memo also states that EWSD switch must be fully certified before recommended fielding of remaining switches		**October 31** Avaya starts testing Definity G3R, rel. 8.2, at JITC			
		November 1 IPTP grants IATO to Army for EWSD, rel. 16, for installation in Mannheim, Germany				**November 3** Nortel starts testing MSL14 at JITC	**November 1** Siemens receives IATO for EWSD, rel. 16, effective Jan 2001–Jan 2002

76

GAO
Accountability * Integrity * Reliability

Appendix II
Timeline (cont.)

			Vendors				
Year	Congress	DOD	AGCS	Avaya	Lucent	Nortel	Siemens
2000 (cont.)		**November 7** Army authorizes installation of Nortel MSL12 in Korea and Japan with Joint Staff approval of JITC test results. Testing completed October 27th, certification letter pending					
		November 8 Army grants Nortel permission to reinstall MSL12 in Qatar		**November 10** Avaya installs uncertified switch at Rock Island Arsenal		**November 14** Nortel begins to install MSL12 switch in Korea and Japan	
			December 2 AGCS installs uncertified upgrade at Fort Gordon			**December 12** Nortel completes installations of MSL12 switch in Korea and Japan	
						December 14–15 Nortel installs certified switch at Spangdahlem, Germany, Air Force base	
						December 26 Nortel receives certification of MSL12	

77

GAO
Accountability * Integrity * Reliability

Appendix II
Timeline (cont.)

			Vendors				
Year	**Congress**	**DOD**	**AGCS**	**Avaya**	**Lucent**	**Nortel**	**Siemens**
2001	**January 3** Senator Warner's staff issues letter regarding Siemens' EWSD switch			**January 4** Avaya installs uncertified switch at Aberdeen Proving Ground			**January 9** Siemens starts testing EWSD, rel. 18, at JITC
	January 18 Senator Warner's staff meets with DOD on interoperability and connectivity process					**January 30** Nortel reinstalls MSL12 at Qatar	
		March 1 IPTP issues IATO to Army for Lucent 5ESS, rel. 14, for Fort Bragg			**March 1** Lucent receives IATO for Fort Bragg, effective Feb 2001–Feb 2002, for 5ESS, rel. 14		
		April 5 Army issues memo eliminating precedence calls for Army units in Europe that do not require this capability. Memo effective for 1-year period ending April 5, 2002					

78

GAO
Accountability * Integrity * Reliability

Appendix II
Timeline (cont.)

Year	Congress	DOD	Vendors				
			AGCS	Avaya	Lucent	Nortel	Siemens
2001 (cont.)		**April 19** JITC issues interim status report on result of EWSD switch testing					
		April 25 General Officers meeting to discuss Siemens' certification status					
		April 27 Army responds to Senator Warner's letter regarding EWSD certification					
		April 27 JITC issues limited certification of EWSD, rel. 18					**April 27** Siemens receives limited certification of EWSD, rel. 18
	April 30 DOD briefs Senators Helms' and Warner's staff on status of DISN-E award and Siemens' switch certification	**April 30** DOD officials brief congressional staff on status of DISN-E award and Siemens' switch certification					
	May 11 Senators Warner and Helms ask GAO to review DOD's certification process and its application of the process						

79

GAO
Accountability * Integrity * Reliability

Appendix II
Timeline (cont.)

			Vendors				
Year	**Congress**	**DOD**	**AGCS**	**Avaya**	**Lucent**	**Nortel**	**Siemens**
2001 (cont.)	**May 25** GAO meets with congressional staff to discuss request						
						June 19 Nortel starts testing MSL15 at JITC	
			June 21 AGCS requests that certification requirements be waived for its switch upgrade based on past performance				
				June 29 Avaya installs switch with IATO at Edgewood Arsenal			
		July 11 DISA requests guidance from Joint Staff on EWSD certification issues					
		July 13 Army appeals EWSD limited certification to IPTP					
		July 17 IPTP surveys military departments regarding capability of EWSD					
.		**July 23** Joint Staff informs AGCS that all DSN switches must be certified			**July 23** Lucent starts testing 5ESS, rel. 15 at JITC	**July 19** Nortel installs certified switch at Capodichino Navy facility in Italy	

GAO
Accountability * Integrity * Reliability

Appendix II
Timeline (cont.)

			Vendors				
Year	Congress	DOD	AGCS	Avaya	Lucent	Nortel	Siemens
2001 (cont.)		**August 1** IPTP survey responses received show that military departments, except Army, do not support global certification of EWSD				**August 2** Nortel installs certified switch at Gricignano Navy facility in Italy	
		August 6 Acting Assistant Secretary of Defense for C3I informs AGCS that certification requirements for switch upgrades will not be waived					
	August 8 GAO meets with Senator Helms' staff to agree on job design (concurrence was obtained from Senator Warner's staff at a later date via e-mail)	**August 10** JITC sends intent to certify e-mail to Avaya for Definity G3R, rel. 8.2, which can be used pending receipt of the certification letter		**August 10** Avaya receives intent to certify e-mail for Definity G3R, rel. 8.2		**August 9** Nortel installs certified switch at Gaeta Navy facility in Italy	
				September 5 Avaya starts testing Definity G3R, rel. 9.2, at JITC			
				September 6 Avaya installs certified switch at Fort Detrick			

81

GAO
Accountability * Integrity * Reliability

Appendix II
Timeline (cont.)

			Vendors				
Year	**Congress**	**DOD**	**AGCS**	**Avaya**	**Lucent**	**Nortel**	**Siemens**
2001 (cont.)		**September 13** DISA on behalf of Air Force issues a work stoppage in Europe that affects General Dynamics and Nortel				**September 13** Nortel distributor (General Dynamics) stops work activities associated with switch installations/ upgrades in Europe	
				September 25 Avaya installs certified switch at Fort Detrick	**September 28** Lucent completes testing 5ESS, rel. 15; certification not received	**September 21** Nortel receives certification of MSL14	**September 26** Siemens ends testing of EWSD, rel. 18
			October 15 AGCS tells GAO it will no longer compete for DOD contracts because of interoperability requirements				

GAO
Accountability * Integrity * Reliability

Appendix II
Timeline (cont.)

			Vendors				
Year	Congress	DOD	AGCS	Avaya	Lucent	Nortel	Siemens
2001 (cont.)	**November 14** GAO meets with congressional staff to provide status update	**November 11** Joint Staff meets with Siemens regarding EWSD certification **November 27** IPTP chairman meets with Siemens regarding EWSD certification **November 30** Joint Staff completes its MLPP study, confirming MLPP as most cost-effective way for DOD to ensure connectivity within the DSN		**December 6** Avaya installs certified switch at Fort McCoy	**November 10** Lucent installs 5ESS, rel. 15, at Fort Bragg without an IATO or certification		
2002		**January 2** Joint Staff validates global use of the EWSD switch with certain restrictions 9 months after JITC issued its certification letter (i.e., limited certification). This validation memo also changed the certification status from limited to global		**January 3** Avaya installs certified switch at U.S. Military Academy at West Point			

83

GAO
Accountability * Integrity * Reliability

Appendix II
Timeline (cont.)

			Vendors				
Year	Congress	DOD	AGCS	Avaya	Lucent	Nortel	Siemens
2002 (cont.)		**January 11** DOD revises directive requiring all IT systems to be interoperable					
		February 1 JITC sends intent to certify e-mail to Avaya for Definity G3R, rel. 9.2, which can be used pending receipt of the certification letter		**February 1** Avaya receives intent to certify e-mail for Definity G3R, rel. 9.2 **February 4** Avaya receives certification of Definity G3R, rel. 8.2			
		February 12 IPTP grants IATO for Lucent 5ESS, rel. 15, effective Feb 2001–Feb 2002		**February 14** Avaya installs certified switch at Fort A.P. Hill			
	February 21 GAO meets with Senator Helms' staff to discuss product type and issuance date (concurrence was obtained from Senator Warner's staff at a later date via e-mail)	**February 19** JITC starts testing of voice over Internet protocol technology with Avaya		**February 19** Avaya starts testing of voice over Internet protocol technology at JITC			

GAO
Accountability * Integrity * Reliability

Appendix II
Timeline (cont.)

			Vendors				
Year	Congress	DOD	AGCS	Avaya	Lucent	Nortel	Siemens
2002 (cont.)	**March 6** GAO meets with Senators Helms' and Warner's staff to discuss product type and issuance date			**March 8** Avaya installs certified switch at Fort Gillem			
	March 25 Senators Helms' and Warner's staff concur to product issuance date change.						
		April 5 Army's memo eliminating precedence calls for Army units in Europe that do not require this capability expires		**April 4** Avaya installs certified switch at Fort Belvoir			

GAO
Accountability * Integrity * Reliability

Appendix III
Abbreviations and Acronyms

AGCS	AG Commercial Systems
C3I	Command, Control, Communications, and Intelligence
CJCS	Chairman of the Joint Chiefs of Staff
DISA	Defense Information Systems Agency
DISN-E	Defense Information Systems Network–Europe
DOD	Department of Defense
DSN	Defense Switched Network
EWSD	Elektronisches Waehl System Digital
IATO	interim authority to operate
IPTP	Interoperability Policy and Test Panel

86

Appendix III
Abbreviations and Acronyms (cont.)

JITC	Joint Interoperability Test Command
Lucent	Lucent Technologies
Nortel	Nortel Networks
PM	program manager
RFI	request for information
SOR	statement of requirements
TDR	test discrepancy report
Telecom	telecommunications
VOIP	voice over Internet protocol

Comments from the Department of Defense

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

June 11, 2002

Mr. Joel C. Willemssen
Managing Director, Information Technology Issues
U.S. General Accounting Office
Washington, DC 20548

Dear Mr. Willemssen,

This is the Department of Defense (DoD) response to the GAO draft report, "INFORMATION TECHNOLOGY: DoD Needs to Improve Process for Ensuring Interoperability of Telecommunications Switches", dated May 13, 2002 (GAO CODE 310215)

We appreciate the opportunity to respond on the subject GAO Report. We have reviewed the report and concur with its recommendations.

While execution of the GAO's recommendations is expected to improve the Department of Defense process for certifying telecommunications switches, we strongly believe that the extant technical approach is sufficient for certifying known telecommunications switches that are connected to the Defense Switch Network (DSN).

The DOD has made every attempt to consistently and fairly apply Interoperability policies and procedures for all switches. In this regard, the findings of the GAO report mistakenly cite the installation of EWSD switches at Funari and Coleman Barracks, Germany as an example of inconsistent application of DOD policies. The instances investigated by the GAO at Funari and Coleman Barracks highlights a situation that involved temporarily connecting switches for test purposes. These switches were not operationally deployed, but were tested in parallel with the existing DSN switch at these locations. This approach did not radically depart from established commercial practices for switch certification testing, and had any failures occurred, an interim authority to operate would not have been granted. At present, the switches remain installed, and have received JITC certification for EUCOM use.

Our consolidated response to the specific recommendations is included in the attached enclosure.

Sincerely,

John L. Osterholz
Director
Architecture and Interoperability

Enclosure

GAO DRAFT REPORT DATED MAY 13, 2002
(GAO CODE 310215)

"INFORMATION TECHNOLOGY: DOD NEEDS TO IMPROVE PROCESS FOR ENSURING INTEROPERABILITY OF TELECOMMUNICATIONS SWITCHES"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: To ensure network interoperability and address the potential impact on competition for telecom switch vendors, the GAO recommended that the Secretary of Defense advance the state of maturity of DoD's telecom switch certification and authorization process by directing the chairman of the Joint Chiefs of Staff; as the DoD authority responsible for the process, to take the following near-term and long-term actions to improve the process.

In the near term,

- use the process flowcharts provided in the GAO's briefing to assist in fully documenting the existing certification and authorization process, and
- make this fully documented process available to DoD and vendor process stakeholders within 60 days.

In the longer term, revise the existing process including switch requirements to ensure that it is complete, current, transparent to stakeholders, and enforceable by the Joint Staff, and issue a revised process to all stakeholders within 180 days. In doing so, the chairman should

- work jointly with the Assistant Secretary of Defense for C31 since this organization is responsible for the interoperability policy and for providing guidance and oversight,
- solicit DoD and vendor input on needed process changes, and
- seek DoD and vendor comments on a draft of the revised process before it is issued in final form. (pp. 2-3/GAO Draft Report)

DoD Response:

Concur.

The Chairman of the Joint Chiefs of Staff will prepare and promulgate a memorandum on the certification process in an attempt to codify and clarify the process for DoD and vendors alike. This memorandum will be officially posted on a Joint Staff Web Site within the next 60 days and remain in effect until incorporated in the next revisions of CJCS Instruction 6215.01B, "Policy for Department of Defense Voice Networks and CJCS Instruction 6212.01B, "Interoperability and Supportability of National Security, and Information Technology Systems."

Additionally, the newly updated DoD 4630.5, "Interoperability of Information Technology (IT) and National Security Systems (NSS)" was approved in January 2002. The newly updated DoD 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and

National Security Systems (NSS)" was approved in May 2002. The new CJCSI 6215.01B, "Interoperability and Supportability of National Security, and Information Technology Systems" was approved in September 2001 and it contains the certification policy. Additionally, the revision processes for CJCSI 6212 and the Defense Switch Network (DSN) Generic Switching Center Requirements (GSCR) have begun and will likewise include clarification of the certification and validation processes as required.

Finally, the Joint Staff recognizes the need to educate the community on switch certification and has taken all the necessary steps to enhance training in this area.

RECOMMENDATION 2: The GAO recommended that the Secretary of Defense direct the Director of the Defense Information Systems Agency, as the DoD authority responsible for certifying the interoperability of switches, to complete its ongoing inventory of installed DSN switches. (p. 3/GAO Draft Report)

Concur.

DISA, at the direction of the Interoperability Policy and Test Panel (IPTP), has completed an initial survey to compile a listing of installed DSN switches. ASD (C3I) will formally direct that all DoD Components submit their current listing of installed DSN switches to DISA. ASD (C3I) will use this as an opportunity to reiterate to the DoD Components that use of the DSN is expressly for military unique applications that require military presence and preemption.

RECOMMENDATION 3: Using the completed ongoing inventory of installed DSN switches, the GAO recommended that the Secretary of Defense direct the Assistant Secretary of Defense for C31, in collaboration with the chairman, to assess the level of DSN interoperability risk associated with having uncertified switches on the network and to develop and implement a risk mitigation strategy to address any risks identified. (p. 3/GAO Draft Report)

Concur.

This assessment was conducted on the initial inventory provided through the IPTP. As a result, the Joint Staff modified the IPTP process to acknowledge switches that have been operational and have posed no known interoperability risk to the DSN. Once the revised inventory is completed, the IPTP will conduct additional assessments and determine what risk mitigation strategies may be required. The Joint Staff will also mandate that organizations desiring to modify their approved connectivity to DSN (by replacing those switches or modifying their software or hardware configurations), inform DISA and the Joint Staff prior to implementing the modifications.

GAO Contact and Staff Acknowledgments

GAO Contact

Cynthia Jackson, (202) 512-5086

Staff Acknowledgments

In addition to the person named above, other key contributors to this report were Naba Barkakati, Harold Brumm, Barbara Collier, Felipe Colón, Frank Maguire, Madhav Panwar, and Teresa Tucker.

GAO's Mission

The General Accounting Office, the investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, managing director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00