United States General Accounting Office

GAO

Report to the Honorable
Craig Thomas, U.S. Senate

December 1999

YEAR 2000 COMPUTING CHALLENGE

Readiness of FBI's National Instant Criminal Background Check System Can Be Improved

GAO
Accountability * Integrity * Reliability

GAO/AIMD/GGD-00-49

Contents

Letter 3

Appendixes

Appendix I: November 19, 1999, Briefing to Senator Thomas 12

Appendix II: Objective, Scope, and Methodology 41

Appendix III: GAO Contact and Staff Acknowledgements 42

Abbreviations

FBI	Federal Bureau of Investigation
III	Interstate Identification Index
IV&V	independent verification and validation
NICS	National Instant Criminal Background Check System
OMB	Office of Management and Budget
POC	point-of-contact

GAO
Accountability * Integrity * Reliability

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

Accounting and Information
Management Division

B-284166

December 16, 1999

The Honorable Craig Thomas
United States Senate

Dear Senator Thomas:

On November 19, 1999, we briefed your office on our review of the Federal Bureau of Investigation's (FBI) efforts to ensure that its National Instant Criminal Background Check System (NICS) is Year 2000 compliant. NICS is an information system that, in concert with other FBI and state-operated systems, is used to conduct presale background checks on persons attempting to purchase firearms. We conducted this review as part of a broader request from your office to review various NICS issues. Because of the time-sensitive nature of the Year 2000 issue, we agreed to brief your office on this issue in advance of completing this broader review.

This report summarizes and updates the information presented at our November 19, 1999, briefing to your staff and provides the Attorney General with recommendations designed to strengthen the Year 2000 readiness of our nation's firearm presale background check program. The briefing slides are presented in appendix I, and our objective, scope, and methodology are in appendix II. We performed our work from September through mid-November 1999 in accordance with generally accepted government auditing standards.

Results in Brief

Two of the most critical phases of the Year 2000 readiness process are testing and contingency planning. Testing is essential to providing reasonable assurance that new or modified systems process dates correctly and will not jeopardize an organization's ability to perform core business operations after the millennium. Contingency planning is needed to mitigate the impact on core business operations of unexpected internal and uncontrollable external Year 2000-induced system failures.

The FBI reported to the Office of Management and Budget (OMB) in August 1999 that NICS was Year 2000 compliant. However, at that time, the FBI did not have a basis for determining system compliance because it had yet to complete system acceptance testing. This testing verifies that an entire system, including application software, system software, and

hardware, performs as intended and thus, is a prerequisite to determining system compliance. As of November 23, 1999, the FBI had not completed system acceptance testing. However, the FBI has defined controls and processes that are consistent with our Year 2000 test guidance for effectively managing system acceptance tests. For example, the FBI has scheduled and planned the tests, prepared test procedures and data, confirmed compliance of vendor services and products, and defined test exit criteria as well as procedures for documenting and managing test results.

The FBI does not plan to end-to-end test the entire set of interrelated FBI and state systems, including NICS, that are needed to conduct firearm presale background checks. According to the FBI, such end-to-end testing is not feasible in the time remaining before the century date change. This conclusion is reasonable given the limited time remaining; however, the FBI is not pursuing alternative, less time-demanding means to minimizing the risks associated with forgoing end-to-end tests with all of its business partners. For example, it is not assessing the Year 2000 readiness of its state partners in combination with defining the scope of an end-to-end test to include only internal FBI systems that support instant background checks of firearm purchasers.

Also, the FBI's draft NICS' Year 2000 contingency plan is missing elements important to ensuring the continuity of instant background check operations. For example, the triggers in the plan are not sufficiently precise to be useful (e.g., the plan identifies persistent capability outage, but it does not define what computer resource capability is degraded and it does not define persistent). Also, the plan does not define the process for training contingency teams on workaround procedures. Further, FBI officials stated that they do not plan to test NICS' contingency plan. Without taking these and other steps, the FBI is unnecessarily increasing the risk that it will not be able to perform instant background checks on prospective firearm buyers' eligibility in the Year 2000. We are making several recommendations to address these issues.

Background

NICS was implemented in November 1998 in response to a requirement of the Brady Handgun Violence Prevention Act of 1993 that background checks be performed on prospective gun buyers. These checks are initiated by federal firearms licensees, i.e., gun dealers, who contact one of two FBI call centers or a designated state point-of-contact (POC) law enforcement

agency and provide information on the buyer (such as name, sex, height, weight, race, and address).

Using these data, the FBI call centers or the state POC access NICS and search three FBI-managed databases to determine whether the prospective buyer is precluded from purchasing the firearm. The databases are: (1) the National Crime Information Center 2000 (NCIC 2000), which contains approximately 700,000 records on wanted persons and subjects who have protective and/or restraining orders, (2) the Interstate Identification Index (III), which is one of three components of the FBI's Integrated Automated Fingerprint Identification System and contains approximately 34.7 million criminal records, and (3) the NICS Index, which contains information provided by federal and state agencies about persons prohibited under federal law from receiving or possessing a firearm.[1] The FBI designated each of these three systems as mission-critical and reported all three as Year 2000 compliant in the Department of Justice's August 1999 Year 2000 report to OMB.

Testing Is Well Behind Schedule But Sufficient Management Controls Are in Place

Complete and thorough Year 2000 testing, including both system acceptance testing and end-to-end testing, is essential to provide reasonable assurance that new or modified systems process dates correctly and will not jeopardize an organization's ability to perform core business operations after the millennium. System acceptance testing verifies that an entire system (i.e., application software, system software, and hardware) performs as intended. End-to-end testing verifies that interrelated systems, which collectively support a core business area, interoperate as intended. OMB required that mission-critical systems be acceptance tested and implemented by March 31, 1999. Justice required that mission-critical systems be tested and implemented by January 1999.

The FBI reported to OMB in August 1999 that NICS was Year 2000 compliant. However, the FBI had not yet conducted system acceptance testing, which is a prerequisite to determining system compliance. The FBI reported NICS as compliant despite not having performed Year 2000 system acceptance testing because the system was designed with a four-digit year date format and because designating it as compliant was consistent with

[1]Records on individuals denied under state law, but not prohibited under federal law, are not to be entered into the NICS Index. Also, any record entered into the NICS Index must be removed if the record is overturned through the appeal process.

Justice guidance for categorizing the Year 2000 status of mission-critical systems.

FBI officials acknowledged that Year 2000 forward date testing should have been completed before the system was implemented in 1998. However, they stated that the NICS' development and deployment schedule did not permit time for such testing before the November 1998 legislatively mandated date for NICS to be operational. They also stated that, after the system was implemented, unexpected operational and performance problems with NICS and the two other FBI systems used in conducting firearm buyer background checks—NCIC 2000 and III—further delayed opportunities for forward date testing. The FBI now plans to complete system acceptance testing in November 1999 and to have a NICS' Year 2000 compliance review conducted by an independent verification and validation (IV&V) contractor in early December 1999.

With little time remaining for conducting system acceptance testing, it is vitally important that the FBI have sufficient controls and processes for managing testing activities. To this end, our Year 2000 test guide[2] specifies, among other things, that organizations should (1) schedule and plan their tests, (2) prepare test procedures and data, (3) confirm compliance of vendor services and products, (4) define test exit criteria, and (5) document and manage test results, including the disposition of defects.

The FBI has defined and is implementing such management controls. For example, its NICS' compliance plan, which it is using in lieu of a test plan, provides for the scheduling and planning of tests. The FBI has also defined test procedures and data, confirmed compliance of vendor services and products, defined test exit criteria, and defined procedures for documenting test results and managing the disposition of defects.

However, the FBI does not plan to end-to-end test all the systems, including NICS, that support its firearm buyer background check program because it believes that it is not feasible to do so at this late date. This position is reasonable at this time given that (1) a NICS' Year 2000 compliance determination is a prerequisite for including a system in end-to-end testing, and this determination is not scheduled to occur until December 1999 and (2) gaining the commitment and securing the participation of multiple external business partners (e.g., states) and scheduling and conducting

[2] *Year 2000 Computing Crisis: A Testing Guide* (GAO/AIMD-10.1.21, November 1998).

such a test would not be possible in the time remaining. Nevertheless, the FBI has not pursued alternative, less time-demanding ways to minimize the risk associated with not conducting end-to-end tests with all of its business partners. For instance, it is not assessing Year 2000 readiness of its state business partners in combination with defining the boundaries of an end-to-end test to include only systems internal to the FBI. Such an approach to end-to-end testing, which verifies that a set of interrelated systems that support a core business function, like presale background checks of firearm buyers, interoperates as intended, is consistent with our Year 2000 test guide.

The NICS Year 2000 Draft Contingency Plan Does Not Include Key Elements

Despite any organization's best efforts to make its mission-critical systems Year 2000 compliant, core business processes are still vulnerable to disruption due to unexpected Year 2000-induced failures and errors in internal systems as well as failures of business partners' systems, or public infrastructure systems, such as power and telecommunications systems. Thus, it is necessary to prepare contingency plans to help mitigate the core business effects associated with these unexpected internal and uncontrollable external system failures.

According to our contingency planning guide,[3] an effective contingency plan should specify, among other things, resource requirements, roles and responsibilities, contingency procedures, and triggers for activating the plan. Consistent with our guidance, Justice requires that contingency plans define, among other things, (1) how long operations can continue in the contingency mode, (2) whether contingency procedures have been verified to ensure that they address the potential scenarios, (3) how contingency teams will be trained on the verified procedures, and (4) how the system will be monitored for correct functioning. Justice also requires that contingency plans be developed and tested by October 1, 1999. The FBI has directed its field and headquarters divisions to test contingency plans by December 15, 1999.

The FBI has developed a Year 2000 contingency plan for NICS. However, this plan does not include several important elements. For example, the triggers defined in the plan are not sufficiently precise to be useful (e.g., the plan identifies persistent capability outage, but it does not define what

[3] *Year 2000 Computing Crisis: Business Continuity and Contingency Planning* (GAO/AIMD-10.1.19, August 1998).

computer resource capability is degraded and it does not define "persistent"). Furthermore, the plan does not define the process for training contingency teams on the verified procedures or procedures for ongoing monitoring of the system for erroneous data.

Finally, while the FBI plans to have the contingency plan reviewed by an IV&V contractor in early December 1999, officials told us that they do not plan to test the contingency plan. The NICS' contingency plan incorporates failure scenarios and operating procedures that, according to FBI officials have been invoked, and thus tested, as part of NICS' normal operations over the last year. Consequently, FBI officials told us that contingency plan testing is not needed. However, the scenarios and procedures that the FBI cited as having been operationally invoked during the year were not Year 2000 in nature. For example, one scenario is for a single state POC to fail. This is a reasonable assumption under normal circumstances. However, it is not as reasonable when applied to Year 2000, given the pervasiveness of the computing problem and the fact that the FBI has not assessed, and thus does not know, the Year 2000 readiness of its state POCs.

Conclusions

The FBI is faced with a compressed and challenging time frame for completing NICS' Year 2000 system acceptance testing and a NICS Year 2000-oriented contingency plan. Moreover, it is increasing risks to its presale background check capability by not pursuing alternatives to end-to-end tests and testing its contingency procedures. Unless it moves swiftly to complete these important tasks, it faces an increased risk of not being able to provide presale background checks of firearm buyers' eligibility in the Year 2000.

Recommendations

To reduce the risk of Year 2000 disruption to NICS and the FBI's ability to perform presale firearm background checks, we recommend that the Attorney General direct the FBI Director to

1. pursue alternative means to minimizing the risks associated with not conducting end-to-end tests with all of NICS' business partners, such as assessing the Y2K readiness of state partners and defining the boundaries of an end-to-end test event to include only internal FBI systems;

2. reflect in the NICS' Year 2000 contingency plan the added risks associated with the FBI's decisions concerning alternatives to conducting end-to-end tests with all business partners; and

3. develop and test the NICS' Year 2000 contingency plan in accordance with our and Justice guidance, including specifying such important elements as precise trigger events and procedures for training contingency teams and monitoring system performance during the rollover period.

Agency Comments

We requested comments from the Attorney General or her designee on a draft of this report. In its comments, Justice stated that the draft report incorporated Justice's and FBI's comments on a draft of the briefing slides that we shared with them prior to our November 19, 1999, briefing to your office. Justice provided no additional comments on the facts, conclusions, or recommendations in this report.

We are sending copies of this report to Senators Robert F. Bennett, Chairman, and Christopher J. Dodd, Vice Chairman, Senate Special Committee on the Year 2000 Technology Problem; Representatives Steven Horn, Chairman, and Jim Turner, Ranking Minority Member, Subcommittee on Government Management, Information and Technology, House Committee on Government Reform; Representatives Constance A. Morella, Chairwoman, and James A. Barcia, Ranking Minority Member, Subcommittee on Technology, House Committee on Science; the Honorable Jacob J. Lew, Director, Office of Management and Budget; the Honorable Janet Reno, Attorney General; the Honorable Louis J. Freeh, Director of the FBI; and the Honorable John Koskinen, Chairman of the President's Council on Year 2000 Conversion. Copies will be made available to others upon request.

Should you or your staff have any questions concerning this report, please contact me at (202) 512-6240. I can also be reached by e-mail at *hiter.aimd@gao.gov*. Other points of contact and key contributors to this report are listed in appendix III.

Sincerely yours,

Randolph C. Hite
Associate Director, Governmentwide
and Defense Information Systems

November 19, 1999, Briefing to Senator Thomas

GAO
Accountability * Integrity * Reliability

Briefing to Senator Thomas on

Year 2000 Computing Challenge: National Instant Criminal Background Check System (NICS)

November 19, 1999

1

GAO
Accountability * Integrity * Reliability

Overview

Introduction

Objective, scope, and methodology

Results in brief

Background

Simplified diagram of NICS architecture

Audit results

Conclusions and recommendations

2

GAO
Accountability * Integrity * Reliability

Introduction

- The Brady Act requires Federal Firearms Licensees (FFL)* to request background checks on all persons attempting to purchase firearms.
- Operational since November 30, 1998, NICS provides access to 3 national databases containing criminal history or other records used to identify persons prohibited by law from receiving or possessing a firearm.

*FFL means a person licensed by the Bureau of Alcohol, Tobacco and Firearms as a manufacturer, dealer, or importer of firearms. There are approximately 93,000 FFLs in the United States.

3

GAO
Accountability * Integrity * Reliability

Introduction

- Senator Thomas asked us to address several issues concerning NICS' operational efficiency and effectiveness, including system performance, architecture, security, and Year 2000 readiness.

- Because of the critical nature of the Year 2000 readiness issue, we agreed to brief the Senator's office on this issue in November 1999.

4

GAO
Accountability * Integrity * Reliability

Results in Brief

- FBI reported NICS as Year 2000 compliant prior to completing system acceptance testing, and it is well behind schedule in completing NICS testing.
- Management of NICS system acceptance testing includes important controls.
- FBI's draft contingency plan does not include several key elements.
- FBI does not plan to test the revised NICS contingency plan.

5

Objective, Scope, and Methodology

Objective

- What efforts has the FBI undertaken to ensure that NICS and its data exchanges are Year 2000 compliant?

Scope and Methodology

- Identified FBI plans and guidance governing NICS Year 2000 compliance.
- Compared FBI plans and actions to date against GAO, Justice, and FBI Year 2000 guidance.*

*Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, November 1998) and Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, August 1998).

6

GAO
Accountability * Integrity * Reliability

Objective, Scope, and Methodology

Scope and Methodology (cont'd)

- Determined FBI progress against plans.
- We briefed the FBI on November 15, 1999, on the results of our review and made recommendations to address our findings. We have revised the briefing, including the recommendations, as appropriate, to reflect the FBI's comments.
- Performed our work from September 1999 through mid-November 1999 in accordance with generally accepted government auditing standards.

7

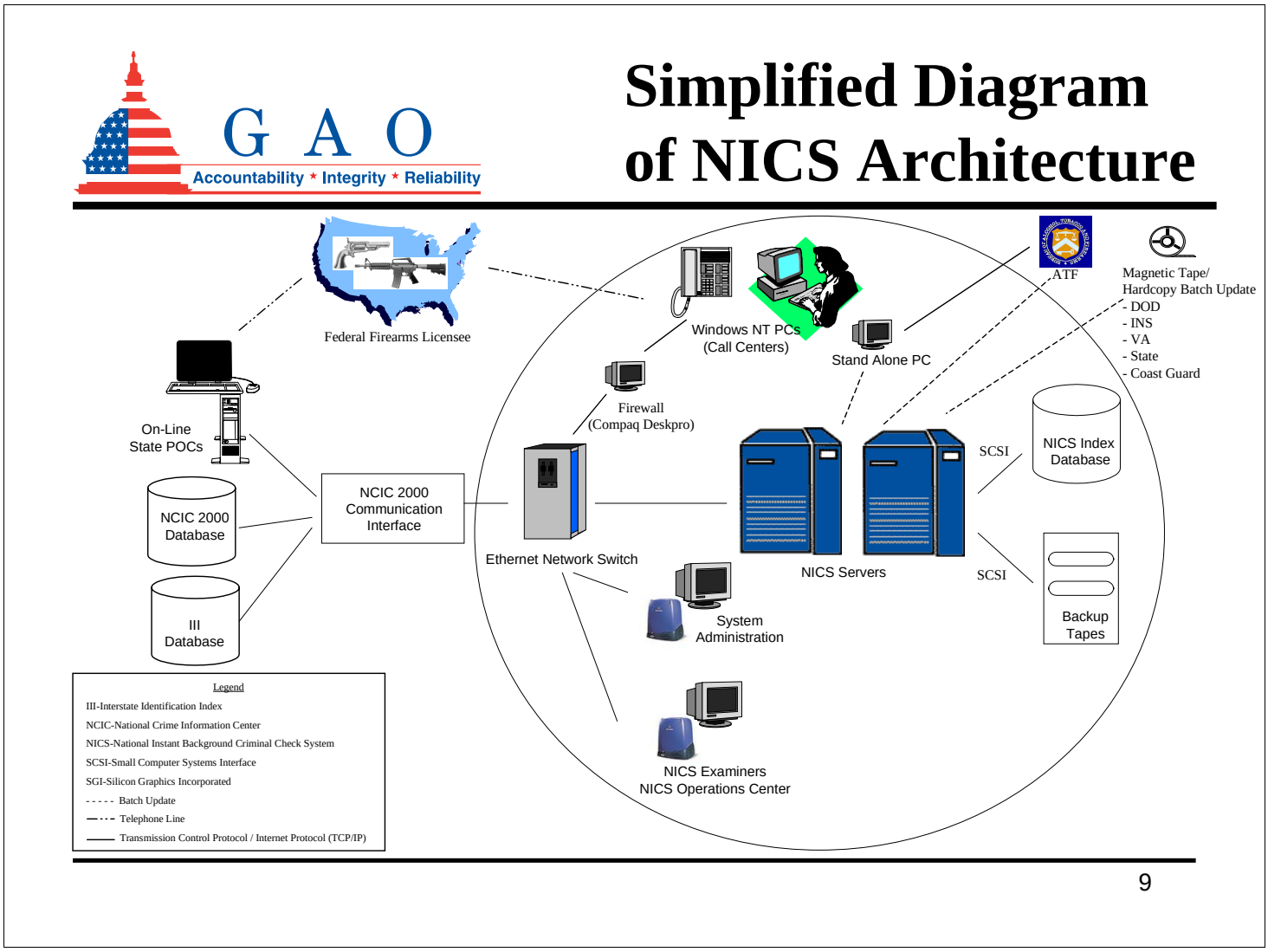
GAO
Accountability * Integrity * Reliability

Background

- In response to FFL queries, NICS searches its own database, referred to as NICS Index, and queries two other FBI databases (National Crime Information Center 2000 (NCIC) and the Interstate Identification Index (III)).
- NICS, NCIC 2000, and III* are 3 of the FBI's 43 mission-critical information systems. All 3 were reported as Year 2000 compliant in Justice's August 1999 report to OMB.

*III database is 1 of 3 components of the Integrated Automated Fingerprint Identification System.

8


GAO
Accountability * Integrity * Reliability
Simplified Diagram of NICS Architecture
Federal Firearms Licensee
On-Line State POCs
NCIC 2000 Database
III Database
NCIC 2000 Communication Interface
Ethernet Network Switch
Firewall (Compaq Deskpro)
Windows NT PCs (Call Centers)
Stand Alone PC
ATF
Magnetic Tape/ Hardcopy Batch Update
- DOD
- INS
- VA
- State
- Coast Guard
NICS Index Database
SCSI
NICS Servers
SCSI
Backup Tapes
System Administration
NICS Examiners
NICS Operations Center
Legend
III-Interstate Identification Index
NCIC-National Crime Information Center
NICS-National Instant Background Criminal Check System
SCSI-Small Computer Systems Interface
SGI-Silicon Graphics Incorporated
- - - - - Batch Update
Telephone Line
Transmission Control Protocol / Internet Protocol (TCP/IP)
9

GAO
Accountability * Integrity * Reliability

Audit Results

FBI reported NICS as Year 2000 compliant prior to completing system acceptance testing, and it is well behind schedule in completing NICS testing.

- Both system acceptance and end-to-end testing are essential components of an effective Year 2000 program.* OMB required that mission-critical systems be validated (acceptance tested) and implemented by March 31, 1999.
- Justice similarly requires such testing, and required that mission-critical systems be implemented by January 1999.

*System acceptance testing verifies that an entire system (i.e., application software and system hardware and software infrastructure) performs as intended and is a perequisite for implementation. End-to-end testing verifies that interrelated systems, which collectively support a core business area, interoperate as intended.

10

GAO
Accountability * Integrity * Reliability

Audit Results

- NICS was reported to OMB as compliant in August 1999. However, the FBI has not yet completed system acceptance testing, which is a prerequisite to determining system compliance. It plans to complete this testing in November 1999 and have its Independent Verification and Validation contractor conduct a system Year 2000 compliance review in December 1999.

11

GAO
Accountability * Integrity * Reliability

Audit Results

- The FBI acknowledges that Year 2000 forward date testing should have been completed before the system became operational in November 1998. However, the FBI stated that the NICS development and deployment schedule did not permit such testing before the November 1998 legislatively mandated operational date. Subsequently, unexpected NICS, NCIC 2000, and IAFIS operational and performance problems delayed forward date testing until now.

12

GAO
Accountability * Integrity * Reliability

Audit Results

- Despite having not performed Year 2000 system acceptance testing, the FBI reported NICS as compliant because it was designed with a 4-digit year date format and designating it as such was consistent with Justice guidance that required systems to be categorized as either “to be replaced,” “to be renovated,” or as “compliant.”

13

GAO
Accountability * Integrity * Reliability

Audit Results

- The FBI does not plan to conduct end-to-end testing because it believes that it is not feasible to do so at this late date. This position is understandable because (1) a NICS Year 2000 compliance determination is a prerequisite for including a system in end-to-end testing, and this determination will not occur until December 1999 and (2) gaining the commitment and securing the participation of external business partners (e.g., states) and scheduling and conducting such a test would not be possible in the time available.

14

GAO
Accountability * Integrity * Reliability

Audit Results

- The FBI has not pursued alternative means to minimizing the risks associated with not conducting end-to-end tests with all its business partners. For example, it has not assessed the Year 2000 readiness of its state business partners in combination with scoping the boundaries of an end-to-end test (which according to GAO's test guide are not fixed but can vary and be defined to reflect an organization's most critical system dependencies) to include only systems internal to the FBI.

15

GAO
Accountability * Integrity * Reliability

Audit Results

Management of NICS system acceptance testing includes important controls.

- Our Year 2000 test guide specifies that effective system acceptance test management includes, among other things:

(1) scheduling and planning the tests;

(2) preparing test procedures and data;

(3) confirming compliance of vendor services and products;

(4) defining test exit criteria; and

(5) documenting and managing test results, including the disposition of defects.

16

GAO
Accountability * Integrity * Reliability

Audit Results

- The FBI has satisfied all of these test management controls:

  (1) NICS compliance plan, which the FBI is using in lieu of a test plan, provides for the scheduling and planning of tests.

  (2) NICS officials stated that they have recently completed test procedures and data.

  (3) NICS officials stated that they have confirmed compliance of vendor services and products.

17

GAO
Accountability * Integrity * Reliability

Audit Results

(4) FBI has defined its test exit criteria as 100 percent passing of all test procedures.

(5) FBI has defined procedures for documenting test results and managing the disposition of defects, which includes prioritizing the defects and analyzing the resources required to correct the problem.

18

GAO
Accountability * Integrity * Reliability

Audit Results

FBI's draft contingency plan does not include several key elements.

- According to our contingency planning guide, an effective contingency plan should specify, among other things:

  (1) resource requirements,

  (2) roles and responsibilities,

  (3) contingency procedures, and

  (4) triggers for activating the plan.

19

GAO
Accountability * Integrity * Reliability

Audit Results

- Justice requires that contingency plans define, among other things:

  (1) how long operations can continue in the contingency mode,

  (2) whether contingency procedures have been verified,

  (3) how contingency teams will be trained on the verified procedures, and

  (4) how the system will be monitored for correct functioning.

20

GAO
Accountability * Integrity * Reliability

Audit Results

- FBI has developed a draft contingency plan for NICS. However, this plan does not include several important elements. For example:
  - The plan describes the supplies and facilities needed to operate in a contingency mode, but it does not describe the necessary staffing and funding to operate in this mode.
  - The triggers defined in the plan are not sufficiently precise to be useful. For example, the plan identifies performance degradation as a trigger, but it does not define the level of degradation necessary to activate the contingency plan.

21

GAO
Accountability * Integrity * Reliability

Audit Results

- The plan does not define:

  (1) how long operations can continue in the contingency mode,

  (2) whether contingency procedures have been verified,

  (3) the process for training contingency teams on the verified procedures, and

  (4) procedures for ongoing monitoring of the system for erroneous data.

22

GAO
Accountability * Integrity * Reliability

Audit Results

- The FBI acknowledges these limitations and told us that it will revise its draft contingency plan. The revised plan is expected to be completed by November 19, 1999.

23

GAO
Accountability * Integrity * Reliability

Audit Results

FBI does not plan to test the revised NICS contingency plan.

- Justice requires that contingency plans be developed and tested by October 1, 1999. The FBI has directed its field and headquarters divisions to test contingency plans by December 15, 1999.
- The FBI plans to revise its NICS contingency plan and FBI officials told us that it will be completed by November 19, 1999. However, the FBI does not plan to test the contingency plan.

24

GAO
Accountability * Integrity * Reliability

Audit Results

- According to the FBI, the revised NICS contingency plan incorporates failure scenarios and operating procedures that have been tested as part of NICS normal operations over the last year, and thus the contingency plan does not need to be tested. The FBI cited such scenarios (e.g., a single state point-of-contact experiences a Year 2000-induced failure) and the procedures that were invoked.
- However, these scenarios and procedures were not Year 2000 in nature. Further, the FBI acknowledges that its has not completed a NICS Year 2000 contingency plan, meaning that it has not fully defined Year 2000 failure scenarios and procedures.

25

GAO
Accountability * Integrity * Reliability

Audit Results

- According to NICS officials, one mitigation to the chance that Year 2000-induced failures would allow ineligible persons to purchase firearms is that FFLs cannot lawfully sell firearms to an individual without a NICS transaction number. FBI's general counsel is currently reviewing this position.

26

GAO
Accountability * Integrity * Reliability

Conclusions

- The FBI is faced with a compressed time frame for completing NICS' Year 2000 testing and developing and testing the NICS contingency plan. Unless the FBI moves swiftly to complete these yet-to-be-completed and important tasks, it faces an increased risk of not being able to provide instant checks of firearm buyers' eligibility in the Year 2000.

27

GAO
Accountability * Integrity * Reliability

Recommendations

To reduce the risk of Year 2000 disruption to this important national program, we recommend that the Attorney General direct the FBI Director to:

(1) pursue alternative means to minimizing the risks associated with not conducting end-to-end tests with all its business partners, such as assessing the Year 2000 readiness of its state business partners and scoping the boundaries of an end-to-end test to include only internal FBI systems;

28

GAO
Accountability * Integrity * Reliability

Recommendations

(2) reflect in its NICS Year 2000 contingency plan the added risks associated with its decisions concerning alternatives to conducting end-to-end tests with all business partners (e.g., multiple state point-of-contact failures); and

(3) develop and test NICS Year 2000 contingency plan in accordance with GAO and Justice guidance, including specification in the plan of such important elements as precise trigger events, resource requirements and allocations, and procedures for training contingency teams and monitoring system performance during the roll-over period.

29

Objective, Scope, and Methodology

Our objective was to assess the FBI's efforts to ensure that its National Instant Criminal Background Check System (NICS) and the systems that it exchanges data with are Year 2000 compliant. To accomplish this objective, we reviewed the FBI's progress toward performing Year 2000 tests on NICS and compared this progress to the Office of Management and Budget (OMB) and Justice milestones. We also identified the FBI's Year 2000 testing management controls and compared these to controls (i.e., key processes) described in our Year 2000 test guide.[1]

We also reviewed the FBI's progress toward developing and testing a contingency plan for NICS and compared it to Justice and FBI milestones. In addition, we identified the FBI's contingency planning management controls and compared these to the key processes specified in our business continuity and contingency planning guidance.[2]

We reviewed the NICS' Compliance Plan (test plan) and contingency plan. In addition, we reviewed Justice's Year 2000-related guidance, including roles, responsibilities, and guidance, dated January 23,1998, and revised October 13, 1999, and its guidelines for testing contingency plans, dated March 1999. To supplement our analysis of documentation, we interviewed Year 2000 program and NICS operations officials and support contractor representatives. We did not independently verify that the FBI's testing and contingency planning controls were functioning as intended.

We performed our work at the FBI headquarters in Washington, D.C., and the FBI data center in Clarksburg, West Virginia. We performed our work from September through mid-November 1999 in accordance with generally accepted government auditing standards. We requested comments from the Attorney General or her designee on a draft of this report.

[1] *Year 2000 Computing Crisis: A Testing Guide* (GAO/AIMD-10.1.21, November 1998).

[2] *Year 2000 Computing Crisis: Business Continuity and Contingency Planning* (GAO/AIMD-10.1.19, August 1998).

GAO Contact and Staff Acknowledgements

GAO Contact

Deborah Davis, (202) 512-6261

Acknowledgements

Scott Binder, Felicia Bradley, Cristina Chaplain, Dan Burton, Madhav Panwar, Mary Lane Renninger, and Dennise Stickley made key contributions to this report.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary, 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

or visit:

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

Orders may also be placed by calling (202) 512-6000
or by using fax number (202) 512-6061, or 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.

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

PRINTED ON RECYCLED PAPER

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

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Rate
Postage & Fees Paid
GAO
Permit No. GI00

[redacted]