SECRET//

Q5 PRELIMINARY ASSESSMENT OF THE NETWORK OUTAGE

(b)(3)-P.L. 86-36
(b)(1)

24-28 JANUARY 2000

4 February 2000

PRELIMINARY ASSESSMENT OF NSA's

NETWORK OUTAGE – 24-28 JANUARY 2000

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

I. Introduction

From 24-28 January 2000, NSA experienced an network outage. This outage effectively prevented from processing collected data This preliminary report is aimed at discussing both the root causes of this outage and other related issues that need to be corrected if the type of outage recently experienced is to be prevented from occurring in the future. The lessons learned from this exclusively event, also apply to NSA's field sites. Even though field campus networks are smaller, and must be equally well supported and managed.

II. Executive Summary

While specific technical problems occurred to cause this outage, when you "peel back the skin of the onion", the causes are rooted in fundamental internal problems related to resources, management, and our ability to implement, maintain, and manage a very complex and large network. There was no evidence to suggest deliberate or malicious activity was involved in this network outage. The technology, vendor equipment, and architectural plans were sound; we simply are not effectively implementing that architecture -- a problem that cuts across organizational boundaries. The solutions to these problems begin with DIRNSA's 100 Days of Change. Resource realignment, centralized management, authority, and accountability, and the stated desire to re-invest in our infrastructure are absolutely essential and are the start of ensuring that the chance of a future outage of this type is minimized.

Approved for Release by NSA on 01-18-2012, FOIA Case # 59324

(b)(3)-P.L. 86-36

III. Lessons Learned Team

Input for this report came from a team of personnel who were personally involved in restoring service as well as individuals who were not directly involved but are customers of services. The full-time team members were:

(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

Additionally the team benefited from the input of:

(b)(3)-P.L. 86-36

IV. Methodology

(b)(3)-P.L. 86-36

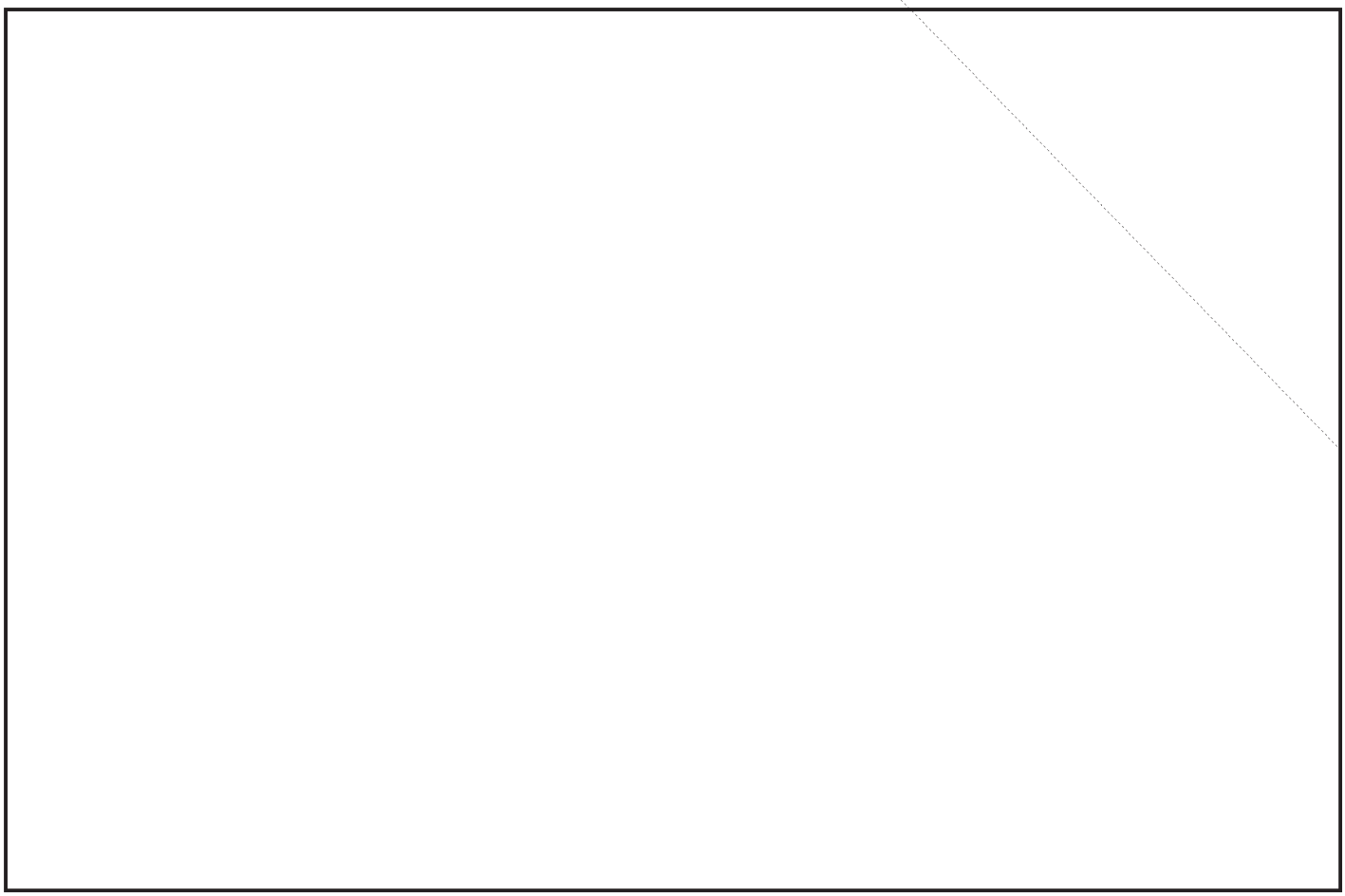
While there is no one single cause of this outage . Through an exhaustive brainstorming session the team recorded all issues and then categorized them into root causes or related issues. The team then discussed the causes and recommended solutions to the problem.

V. Root Causes (Priority Order)

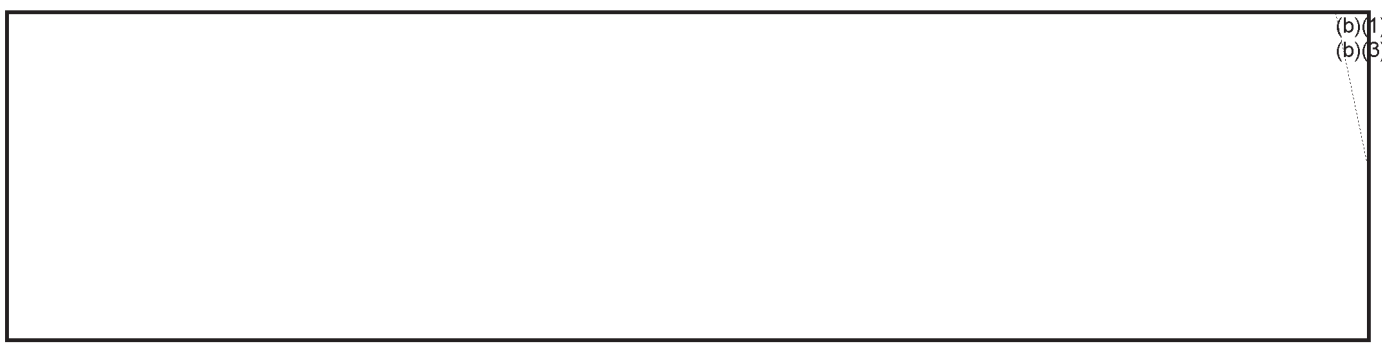
(b)(1)
(b)(3)-P.L. 86-36

a. **Resources**: Throughout the discussion of root and related causes, there is one fundamental, overarching root cause – lack of resources in terms of dollars and manpower.

(b)(3)-P.L. 86-36

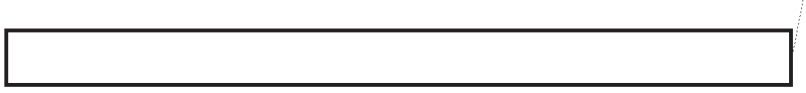


Of particular concern is the need to increase the level of skilled government and contractor manpower, to retain skilled government and contractor manpower, and to train network professionals. Skilled government network professionals who understand the SIGINT system are critical to NSA's future.



Solution:

Short Term: DIRNSA has embarked on many significant initiatives to improve NSA's business practices by setting corporate priorities and aligning funding according to those priorities. The decision to consolidate IT into a single NSA organization will not only bring centralized management and accountability to IT, but also eliminate the duplication of some efforts and allow management to better focus scarce resources. In June 2000, DIRNSA will make a decision on outsourcing (GROUNDBREAKER). The results of that decision will directly effect network resources. This network outage illustrates the inextricable link between our information infrastructure and our core business.



Long Term: IT and networks must have an adequate and sustained level of resources. If network services are not outsourced in part or in their entirety, serious attention must be given to hiring, retaining, and training Government network experts. Additional vendor experts will also be required but the exact level of manning is undetermined at this time.

(b)(3)-P.L. 86-36

ACTION TAKEN: Senior NSA management is addressing the issues of funding and personnel. The current DT restructuring will resolve many of the organizational issues and provide a single decision-making authority for networking issues. An independent external team consisting of [redacted] and other industry experts has been commissioned to review the [redacted] network. This team will make substantive recommendations by 15 March 2000 on architecture, upgrades, network stability, and resource issues. An internal team is being established to review the recommendations and develop a plan to implement these recommendations.

b. **Lack of Management Action:** Most of the findings of this review group have been known and discussed many times, in many forums. However, little significant change has occurred to date. Resource problems are well known. Many of the things that need to be done to improve the network are well known. An NSA Office of Inspector General ITI Survey conducted 4 October 1998 to 16 March 1999, revealed similar problems. Also of particular concern to this review team is that their management is in many cases ignoring recommendations of technical experts.

Why the Problem Occurred: Corporate processes and management have not properly prioritized NSA's needs, including infrastructure, to fund those priority items and say no to those not funded. NSA has been downsized in terms of resources (dollars and personnel) but it has not cut mission. Meanwhile, the SIGINT environment is radically becoming more challenging. As for technical recommendations being ignored, in some cases this is true. In the broad, complex, and quickly changing field of telecommunications and networks, senior managers must rely on the input of technical personnel.

Solution:

Short Term: DIRNSA has embarked on many significant changes in an effort to change the way NSA manages its business to allow us to begin corporately addressing NSA priorities and aligning funding according to those priorities. He has engaged DoD, the IC, and Congress and is soliciting their support for these changes and additional resources. The management team will change with the centralization of IT and networks and managers will fully take advantage of their qualified technical workforce.

Long Term: The changes started by the DIRNSA must come to fruition.

ACTION TAKEN: The centralization of IT and networks and their consolidation into a single NSA organization will not only bring centralized management and accountability to IT, but will enable informed decision making for the entire network, not just the backbone or user network portion. This decision making will include funding, manpower, and technical issues.

c. **Culture Change**: NSA must recognize the fundamental importance of the IT infrastructure and in particular the network undercarriage. The network is complex, requiring highly skilled experts to plan, implement, and manage. Serious senior management attention must be given to the importance of the network and its resource demands. An appreciation for the

infrastructure must be a factor considered by all levels of management in making business and operational decisions. In fact, NSA must learn what most successful businesses have learned: that IT, in particular the network, is absolutely vital to their business. Our business processes must also change. Budgets for IT technology must be allowed to be soft on specifics in the out-years, because the rate of change in technology makes accurate predictions on required specific changes impossible. In addition, our current network procedures and management tools reflect our past non-networked world or "the CLOVER way of doing business." They must be reexamined.

Why the Problem Occurred: Culture is developed over time as a result of the environment the organization is operating in. This environment influences behaviors both organizationally and individually. These behaviors become our culture; changing our culture will take leadership, vision, and time.

Solution:

Short Term: DIRNSA's 100 days of change is the beginning. The reorganization of IT and networks is the next step.

Long Term: NSA must partner more closely with commercial network vendors to adapt our procedures to a highly complex, vitally important, and dynamic network environment.

ACTION TAKEN: An independent external team has been commissioned that will make recommendations to senior management based upon their findings and industry practices. In addition, an internal team will be commissioned to review our practices and procedures and will jointly make recommendations. Senior management must incorporate these findings into the NSA culture and foster these cultural changes into the workforce.

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

Why the Problem Occurred: There are several reasons for this problem. [redacted]

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

Solution:

Short Term: [redacted]

[redacted]

Long Term: An effective network performance management capability must be established. NSA must set aside or acquire a cadre of highly skilled network engineers to routinely monitor the performance of the network. Based on this data, network upgrades can be planned, and potential network bottlenecks averted and problems prevented.

ACTION TAKEN: A cross-organizational team of technical experts, planners, implementers, customers and contractors has been established to address technical issues that arise due to architecture, installation, network operations and management, or user issues. This team has met bi-weekly since December 1999 and has been successful in resolving technical problems with the input of the affected organizations.

(b)(1)
(b)(3)-P.L. 86-36

e.

Solution:

(b)(1)
(b)(3)-P.L. 86-36

Short Term: Investigation as to why this event occurred must continue. The effort to perform a complete review may help determine the cause and will reveal if there are any

ACTION TAKEN: A cross-organizational team has been convened to assess the current configuration management processes for the network, as well as to make recommendations for improvements to these processes. This team will also commission a review of the implementation of the network to verify the compliance with the approved architecture and other conditions that could precipitate breakdowns. This assessment will be completed by mid-March.

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]

[redacted]

Solution:

(b)(1)
(b)(3)-P.L. 86-36

Short Term: [redacted] Urgent network upgrades must take precedence and network downtime scheduled if required. It is essential that we develop the core and area infrastructures to the point where these types of upgrades can be accomplished without having to request downtime. The infrastructure needs to be robust enough to perform these functions transparently to the users.

ACTION TAKEN: A detailed Action List was generated as a result of the internal [redacted] Network Review Team Report published 22 December 1999. These actions make specific recommendations for hardware and software upgrades to the network and for new hardware and technology to be inserted into the network; address documentation of network services; and address configuration and performance management and process definition. The cross-organizational team will schedule completion dates for these actions.

g. **Network Responsibility is Fragmented**: There is no one senior manager responsible for NSA's network. DT is responsible for the campus backbone networks, while other Key Components are responsible "their" user networks. As a result, decisions are consensus-driven and overly complicated, and procedures are inefficient.

Why the Problem Occurred: We have evolved to this point as several past organizational realignments have caused this problem and reorganizations have neglected processes.

Solution:

NSA will consolidate IT functions into a centralized IT organization by 1 March 2000. This IT organization will likewise have a centralized network organization that brings together, under a single office-level manager, all responsibility for networks from architecture development, to planning, to implementation, to operations and maintenance for both user backbone networks. This will improve accountability, streamline decision-making, and facilitate procedural changes.

ACTION TAKEN: The reshaping of DT will consolidate IT across the agency and the further consolidation of networks in a single organization will solve this problem.

VI. Other Observations

(b)(3)-P.L. 86-36

[redacted]

While many of these observations have as their root causes those items described above, the following adds some additional specifics.

(b)(1)
(b)(3)-P.L. 86-36

a. **Maintenance**

[redacted]

[redacted] Lack of skilled technicians along with lack of standard procedures and quality control seriously degrades effective network fault isolation and correction.

Solution: Add resources to increase levels of support and maintain technical skill level.

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

Solution: None at present; however, we will continue to work with industry and our own modeling and simulation experts to develop proposals to resolve this problem.

[redacted]

b. **Architecture**

(b)(1)
(b)(3)-P.L. 86-36

Observation: An out-of-band management capability may have future benefit to network operations and maintenance.

Solution: Use of out-of-band has its advantages and disadvantages. A requirement study and cost/benefit analysis is needed.

[redacted]

(b)(3)-P.L. 86-36

[redacted]

Solution: Requires further study and a total SIGINT system approach to determine [redacted] (b)(1) (b)(3)-P.L. 86-36

Observation: Network performance can be improved by performing the "right functions on the right equipment". While not contributing to this particular problem, this and many other upgrades are planned pending availability of commercial equipment and funds.

Solution: Fund identified network upgrades.

Observation: It takes too long for NSA to test new software versions.

Solution: While related to lack of resources, it is also a configuration management issue as to how much testing is required for commercial software. A separate configuration management group is being commissioned to address the entire scope of network configuration management.

Observation: Network plans are not well communicated among all involved parties.

Solution: Centralization of network functions will facilitate communications and network planners will keep all stakeholders engaged and informed.

(b)(1) (b)(3)-P.L. 86-36

c. **Contingency Planning**

[redacted]

[redacted]

d. **Crisis Response**

Observation: During this extended outage, the network Crisis Action Cell (CAC) proved useful but should have been set up earlier. Users and other interested parties (e.g. partners) had difficulty obtaining information as to the status of the network or other pertinent information and often got conflicting information.

Solutions: At all levels who is in charge needs to be clearly understood. Clear lines of authority and accountability needs to be established.

e. **Network Monitoring** (b)(3)-P.L. 86-36

Observation: [redacted]

(b)(3)-P.L. 86-36

[redacted]

[redacted]

f. **NSA/Contractor Strategic Partnerships** (b)(1) (b)(3)-P.L. 86-36

Observation: NSA needs to strengthen the relationship with its network vendors, whereby the contractor better understands NSA needs and NSA better utilizes the vendor's expertise and benefits from commercial practices.

Solution: Expanded relationships should be explored and contracts amended to attain a level of partnership that results in "co-ownership".

[redacted] (b)(1) (b)(3)-P.L. 86-36

VII. Positive Observations

While there are many challenges that must be addressed in order for NSA to have a "best in class" network infrastructure. This outage did underscore several important positive aspects that must be iterated.

Observation: **There Was No Inherent Problem with the Technology** [redacted] This crisis was not caused because [redacted] is not the right technology. [redacted]

Observation: **There Were No Inherent Problems with Vendor Equipment** [redacted] This crisis was not caused by latent software bugs or hardware malfunction. It was also not caused by having [redacted] equipment in the network. (b)(3)-P.L. 86-36

Observation: **No Evidence of Malicious Action**. A first-look analysis of the network outage by C4 revealed that there was no evidence to suggest that deliberate or malicious activity was involved in the network outage.

Observation: **NSA Received Outstanding Vendor Support**. NSA greatly benefited from the support of [redacted] Additional emergency shipments of equipment were made without question. [redacted] brought significant manpower resources to bear on the problem, not only to ascertain the problem but then to implement required changes throughout our infrastructure in an extremely short time frame.

Observation: **Outstanding Teaming**. Once again, in times of crisis, everyone puts personal agendas aside. The cooperation between [redacted] was particularly noteworthy and

(b)(3)-P.L. 86-36

[redacted]

the team of contractor and government personnel from multiple organizations worked with singleness of purpose – restore the network, restore SIGINT. (b)(3)-P.L. 86-36

Observation: **The [redacted] Physical Architecture is Sound**. This crisis was not caused by a flaw in the physical architecture. The physical architecture when fully implemented provides for [redacted] Although there were core problems, this is not an architectural shortcoming. As technology and the network evolve, the architecture requires periodic re-examination.

Observation: **Needed Network Upgrades Were Known**. There were no network modifications made that were not already known to network planners. NSA's ability to implement those modifications was hampered for the reasons described above. Many planned upgrades were installed during the downtime, the logical architecture was altered and processor upgrades were performed.

[redacted]

SECRET [redacted]

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

[redacted]