SECRET [redacted]

(U) Steering Committee Final Report

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

Directors Note to DCI
Cover Signatures
Executive Summary
Introduction and Participants
History/Chain of Events/Recovery
Future IT Plans
Policies, Processes, and Practices
Conclusions and Recommendations

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

(U) Executive Summary

(S [redacted] network outage occurred at NSA in January 2000. It effectively prevented [redacted] from processing collected data [redacted] The fundamental problem leading to this outage was management [redacted] the technical issues were the result of the management problems.

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

(S [redacted]) The [redacted] failure in question characterizes a wider managerial deficiency within NSA. [redacted]

(S [redacted]) The specific event that triggered network instability and the subsequent outage is still subject to investigation, but the technical reason for the problem was [redacted] As a result, the technical problems leading to the outage were not recognized, and correction of the outage took too long.

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

(C [redacted]) The underlying management problems that led to the situation, however, had been recognized and documented for several years prior to the outage; the outcome should not have been a surprise to anyone involved. Authority was distributed across a number of organizations, [redacted]

(U//FOUO) A very different management approach is needed to minimize future difficulties, and it must include a centralized Information Technology Infrastructure (ITI) organization that manages the ITI. This organization must simultaneously be responsive to changing consumer needs, plan its investments in IT modernization carefully, and manage its operations to

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

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

[redacted]

achieve documented service level agreements. It must be structured to achieve those requirements (not subordinated to DT), and it must be supported by highly disciplined formal policies and procedures that allow it to function appropriately. DIRgram-65 is a step in the right direction, however the current directive does not go far enough.

(U//~~FOUO~~) Formal policies must be adopted to clarify the relationship and authority of this new organization to avoid the problems of the past and allow it to perform its functions according to the IT Business Plan. These policies must ensure funding as well as centralizing decision-making, and they must be designed to use appropriately skilled personnel effectively. One alternative involves some degree of outsourcing, but that topic is being separately addressed and was not a subject of this study.

(~~S~~) Both the technical and underlying management problems of the IT Infrastructure are solvable.

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

1. (U) Introduction and Participants

(U//~~FOUO~~) This Independent Industry Review of the Information Technology Infrastructure was undertaken in response to a request by Mr. George J. Tenet, Director of Central Intelligence, on 3 February 2000. The request was triggered by unplanned outage of the computer network at during 24 – 28 January 2000. Because the computer network is an integral part of the Information Technology Infrastructure, this review focused on the network but also addressed the larger issue of the entire IT Infrastructure. (b)(3)-P.L. 86-36

(U//~~FOUO~~) The review included interviews with many of the participants in correcting the outage as well as examining extensive documentation. The interviews and examination were largely done by representatives from However, representatives from additional industrial organizations participated and contributed their insights. Appendix A is the report from which lists the individuals who participated in this review, and it presents the detailed findings of that review. Appendix B provides an initial assessment of the situation written shortly after restoration of service. Appendix C presents an assessment of the outage's impact on the Intelligence Community.

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

2. (U) History/Chain of Events/Recovery

(~~S~~) The network outage began on January 24 in the network infrastructure. The outage was caused by Diagnosing the problem and taking corrective actions required over three days;

(~~S~~) A variety of problems might cause so identifying the probable cause was difficult. Initially, technical personnel believed the problem involved a and took actions appropriate

to that situation [redacted]

(S [redacted]

(S [redacted]) The specific event that triggered the network instability [redacted]

(U//~~FOUO~~) The successful alternative was to [redacted]

(S [redacted] At that point, network services were restored.

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

(S [redacted]

(S [redacted]

(C/ [redacted]) Most of the above issues had been previously identified by both the network technical personnel and by the Office of the Inspector General; the result should not have come as a surprise. Those issues have grown in an environment where mission readiness has had a much higher priority than modernization – or even maintenance. [redacted]

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

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

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

(U) The situation is analogous to an individual who purchases a new automobile, but has too many day-to-day activities to take the car into the gas station to have the oil changed. Such a compromise with best practices (getting the oil changed on schedule) can work fine for a few days, but not for a year or two. After a long enough period, the car begins to malfunction and its exhaust pipe emits lots of smoke. Those are warnings to get maintenance done – and not to drive too fast or be too dependent on that vehicle. Good diagnostic equipment is needed to find out the extent of possible damage and then get it fixed.

(S) Probably even more importantly, no management structure was in place to ensure that actions necessary to achieve stability were undertaken (in addition to giving responsive consumer support). Inadequate emphasis was placed on infrastructure efforts as a result of the unbalanced management structure. This imbalance was great enough that successful restoration of network functionality must be considered only a first step toward recovery.

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

3. (U) Future IT Plans

(S) Although the network is currently back in operation However, avoiding future problems will require correcting the existing unbalanced management structure and dramatically increasing operational discipline.

(S)

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

(S)

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

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

[redacted] The current architecture should be reexamined in light of the outcome of the industry trends. (b)(3)-P.L. 86-36

(U//~~FOUO~~) [redacted] Some progress has been already been made in this regard, but considerably more needs to be accomplished. Of course, routine procedures need to be used with these tools, and personnel need to be trained in their use. Simply having those tools will not be adequate: management structure, policies, and practices must be in place to ensure that they will be used in appropriate ways.

(U//~~FOUO~~) Initial plans for making the needed management changes have already been announced. In DIRgram-65, sponsored by the Agency CIO, the Director of NSA (Lieutenant General Michael V. Hayden) announced that the IT infrastructure would be managed centrally, and that it (and its personnel) would report to the Deputy Director of Technology and Systems. The resulting organization will be responsible for the networks, the data centers, the distributed computing, the telephony system, the enterprise management, and the system engineering of the infrastructure. The change to Enterprise-wide management of the IT Infrastructure will be wrenching for many people involved; it will require elevating the organization and making major changes in processes and values. The NSA CIO has produced an initial IT Infrastructure Business Plan to guide the governance of the resulting ITEG (Information Technology Enterprise Group). (b)(3)-P.L. 86-36

(U//~~FOUO~~) Governance processes were designed for the ITEG to change decision-making practices to a centralized focus. [redacted] Therefore, a centralized System Engineering Organization is planned for dealing with enterprise-wide IT issues and to support a new governance process.

(U//~~FOUO~~) The planned governance process is very similar to the approach used in many industrial and commercial organizations. They have found that centralization of authority for infrastructure is necessary – but with the needs of consumers always being respected and considered. Many firms have centralized their IT authority and established a "users' guidance board" to set policy and monitor progress. At NSA, the importance of IT is even greater than in commercial organizations and has led to dividing the governance into three parts. Each of the resulting Boards emphasizes a different aspect of the IT Infrastructure: (b)(3)-P.L. 86-36

- ☐ (U//~~FOUO~~) [redacted]
- ☐ (U//~~FOUO~~) [redacted]
- ☐ (U//~~FOUO~~) [redacted]

(U//~~FOUO~~) The governance process is purposely not aligned with individual organizations. The intent is to provide a mechanism for encouraging the adoption and successful implementation

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

[redacted]

of practices that reduce arbitrary differences. Without these differences, effort can be concentrated on improving stability, performance, and cost-effectiveness. [redacted]

(U//~~FOUO~~) [redacted] reviewed the documented IT Infrastructure Business Plan. Their observation is that "The overall business strategy is correct, 'right on'." However, they also observe that "Organizational (cultural) change issues are recognized as a barrier. This cannot be overemphasized."

(U//~~FOUO~~) The concern with problems of "culture" (sometimes called "organizational values") are also recognized by both NSA employees and the Independent Industry Review Team. The issue has been addressed in the March-April 2000 issue of *Harvard Business Review* where the authors state "Despite beliefs spawned by popular change-management and reengineering programs, processes are not nearly as flexible or adaptable as resources are – and values are even less so. So whether addressing sustaining or disruptive innovations, when an organization needs new processes and values – because it needs new capabilities – managers must create a new organizational space where those capabilities can be developed."

(U//~~FOUO~~) The challenge for NSA management is to institute the needed cultural change – either through the "new organizational space" of the ITEG or through out-sourcing. In either case, new policies, processes, and practices must be instituted to achieve the necessary results.

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

4. (U) Policies, Processes, and Practices

(U~~//FOUO~~) Policies, processes, and practices must be put in place for the ITEG to achieve success in improving the IT infrastructure. These must clarify relationships and degrees of authority so that necessary actions can be undertaken. [redacted]

(U~~//FOUO~~) Based on the report of the Independent Industry Review Team and additional knowledge of the situation, the Steering Committee concluded that significant changes are required in policies, processes, and practices involving the IT infrastructure. Required policies, processes, and practices for computer networks overlap significantly with those for other areas of the IT infrastructure, so the recommendations below apply across the entire IT infrastructure. These only deal with a few of the needed changes, but they are especially important [redacted]

(U) Policies

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

[redacted]

(U//~~FOUO~~) The policies recommended below are needed to correct problems in managing the IT infrastructure at NSA. They need to apply Agency-wide.

(U//~~FOUO~~) Policy 1: Modernization and maintenance activities will be accorded the priority needed to maintain long-term readiness,

(U) Processes

(U//~~FOUO~~) Processes are needed to ensure adherence to these policies and to correct dysfunctional practices. These include the following:

(U) Practices

(U//~~FOUO~~) The practices of personnel, the way they go about doing their jobs, reflect the values of the organization. Current practices emphasize responsiveness to mission requests, lack of formal guidelines, and on-the-job training. Significant revisions in practices are needed.

[redacted]

5. (U) Conclusions and Recommendations

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

(U//~~FOUO~~) As demonstrated by the January outage, the success of NSA is dependent on its Information Technology Infrastructure. The conclusion of the Independent Industry Review Team is that deep technical issues were not at the core of the outage; the underlying problems were related to management. The technical problems can be solved, but appropriate policies and processes must be put in place to ensure success.

~~(S~~ [redacted]

(U//~~FOUO~~) The underlying management problems must be cured. The Independent Industry Review Team concluded that the lack of an effective enterprise approach to managing the IT infrastructure was its most important observation. The Independent Industry Review Team Steering Committee recommends, in response, that:

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

- ☐ (U//~~FOUO~~) Management of the IT Infrastructure be centralized as defined in the IT Business Plan, [redacted]
- ☐ (U//~~FOUO~~) Outside experts be used to review the mission & function and organization of the ITEG. Special emphasis should be paid to the issue of clear lines of authority, non-overlapping functions, and adoption of industry best practices. Implementation of the recommendations should be made mandatory.
- ☐ (U//~~FOUO~~) Formal policies, processes, and practices (like those presented above) be in place to ensure the ITEG functions effectively as a service provider.

[redacted]

- ☐ (U//~~FOUO~~) Technical and management reviews be performed on an annual basis (with reporting to the CIO) to ensure that appropriate policies, processes, and procedures are being executed. The first such audit be performed in June 2000.

(U//~~FOUO~~) The specific findings of the Independent Industry Review Team are as follows:

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

[redacted]

- (U//~~FOUO~~) Despite broad authority, to date, the NSA CIO function has not been successful in managing the NSA IT Enterprise as an Enterprise
- (~~C~~ [redacted]) While the CIO has significant authority, others also have authority over IT resources. These overlapping authorities often work at cross-purposes.
- (~~C~~ [redacted]) There is no overarching IT Enterprise Plan. [redacted]

- (U//~~FOUO~~) There is no Enterprise-wide IT Infrastructure organization

[redacted]

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

- (U//~~FOUO~~) Currently, ITEG is not an Enterprise-wide organization

[redacted]

- (U//~~FOUO~~) Consolidation of IT resources, even in ITEG, is not by itself sufficient. The

[redacted]

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

- We saw little evidence of accountability in our review. Rather, there is a tendency to attribute every problem to a lack of resources.
- It is not clear that the current ITEG construct increases accountability.

[redacted]

(U//~~FOUO~~) The specific recommendations of the Independent Industry Review Team are as follows:

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

[redacted]

- (U//~~FOUO~~) NSA has never been managed as an IT Enterprise, and accountability in managing the Enterprise is key. Cultural change and transformational leadership are necessary to make the IT Enterprise work. [redacted]

[redacted]

- (U//~~FOUO~~) A detailed IT Enterprise plan, to guide IT Infrastructure decisions toward the

[redacted]

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

Enterprise level, is essential. *We recommend the Director, NSA mandate development of such a plan by the CIO and the new Chief, ITEG, within 90 days.*

☐ (C) To support effective planning, NSA's IT Infrastructure must be based on validated mission requirements – and these requirements must be prioritized.

SECRET

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

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