



May 17, 1985

Mr. Daniel Nauer
Aerospace Industries Association
1725 DeSales Street N. W.
Washington, D. C.

Dear Mr. Nauer:

The following recommended response to the Draft Defense Investigative Service Industrial Security Letter (ISR) entitled "Computer-Based Access Control Systems" which was circulated for industry comment is furnished for your consideration as a CODSIA response.

The rationale reflected in the DIS policy that electronic bits of data (which identify a particular person seeking entry to a controlled area) passing over transmission lines from push-button access control devices to a central processor, require the same protection as combinations to classified containers, is a major obstacle to cost effective use of automated access control systems. This single determination (that these bits are classified) then leads to the requirement that the entire system must be protected as classified under the provisions of Chapter 13 of the Industrial Security Manual (ISM) and particularly paragraph 109 concerning the need for hardened line protection. It is the consensus of the industry respondents to the draft ISR that this standard exceeds reasonable physical security requirements for access control systems and ignores the numerous other protective security measures built into virtually all automated access control systems. The application of the same standards for protecting unattended containers storing classified material, to need to know access to occupied controlled areas is not realistic. Both government and industry would be better served by ensuring that occupants of controlled areas fulfilled their responsibilities for establishing the need to know access of persons entering the area rather than condemn all automated access control systems to meeting such stringent criteria.

It was also the consensus of respondents that it was counterproductive to publish the ISR as current policy before the NISAC Access Control Subcommittee met to consider alternatives to these policies. The ISR is after all an interpretation of the existing policy already published in

On file OSD release instructions apply.

Federal Systems Group
Sanders Associates, Inc., 95 Canal Street, Nashua, New Hampshire 03061 (603) 885-
Telex 094-3430 TWX 710 228-1894

Approved For Release 2006/01/12 : CIA-RDP96B01172R000100040004-4

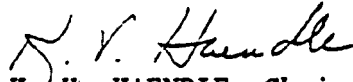
 SANDERS

the ISM. In this case the interpretation leans heavily on security practices that were intended to protect sensitive classified information on automated data processing systems.

In summary, the general reaction to the proposed article in the ISR was surprise that the interpretation of the ISM policy was so strict when applied to guidelines for DIS approval of automated access control systems. None of the respondents considered the policy as stated in the ISR to be reasonable or justified when applied to existing state of the art access control systems. Nearly all of the respondents were acquiring or planning to acquire an access control system and expressed the hope that new, less restrictive guidelines could be resolved as early as possible.

If there are any questions regarding responses from industrial security representatives, please contact me at (603) 885-5510.

Sincerely yours,



K. V. HAENDLE, Chairman,
CODSIA Subcommittee on Automated
Access Control Systems

AP-SEC 85-10
May 1, 1985

AEROSPACE PROCUREMENT SERVICE MEMORANDUM

TO: Industrial Security Committee

SUBJECT: Proposed Industrial Security Letter (ISL):
Computer-Based Access Control Systems

Attached is a copy of the proposed ISL on Computer-Based Access Control Systems. A CODSIA Task Group on Automated Access Controls, chaired by Vic Haendle of Sanders Associates, has been working on this issue for the past year or so. Because of the May 8, 1985 deadline, your comments should be phoned to Vic at 603/885-5510. He, in turn, will coordinate and relay your comments to the Defense Investigative Service.



Daniel J. Nauer

cc: Industrial Security Mailing List
CODSIA

DRAFT 156

COMPUTER-BASED ACCESS CONTROL SYSTEMS

The utilization of computer-based access control systems as supplanting or supplemental devices for closed or restricted areas must receive the approval of cognizant security offices (CSO's) prior to installation. To assist contractors in determining whether proposed systems will meet CSO approval, the following guidance, used by DIS in evaluating proposed access control systems, is provided for information:

If a computer-based access control system has remote entry points, the transmission lines between the central processor and remote card reader/push-button devices at closed or restricted areas must be protected in accordance with paragraph 109 of the Industrial Security Manual. Codes encrypted by methods which conform to the National Bureau of Standards, Data Encryption Standard (DES), or any other commercial encryption method, still require line protection.

A single system may control multiple areas (both controlled and uncontrolled). However, if a system is used for access to a controlled area, the controller (processor and storage) is subject to Section XIII, Industrial Security Manual provisions for continuous protection.

These systems can be approved for access control to controlled areas during working hours only. Normal security provisions apply for non-working hours.

Remote card reader/push-button devices used to obtain entry to controlled areas must conform to paragraphs 36a(2)(a), (b), and (d) of the Industrial Security Manual.

For entry to controlled areas, these devices must use either a push-button combination or a control card used in conjunction with a push-button combination. Paragraphs 36a(1)(b) and (c) on control of combinations apply. The provisions of 36a(1)(a), (b), and (d) of the Industrial Security Manual.

The rapid and continuing advancements in automated access control systems has been recognized by the National Industrial Security Advisory Committee (NISAC) and DIS as an area to be examined to ensure the currency and adequacy of industrial security policy pertaining thereto. To this purpose, a NISAC subcommittee has been established to review the characteristics and applications of automated access control to the DISP. A similar task group has also been formed by the Council of Defense and Aerospace Industries Association. We solicit your thoughts and recommendations for the improvement and update of industrial security policy governing automated access control as outlined above and in paragraph 36 of the ISM.