

FORMAL STATEMENT

J. William Leonard

Director, Information Security Oversight Office

National Archives and Records Administration

before the

Committee on Government Reform

U.S. House of Representatives

May 6, 2004

Chairman Davis, Mr. Waxman, and members of the Committee on Government Reform, I wish to thank you for holding this hearing on security clearance backlogs and reciprocity issues for defense industry personnel and for inviting me to testify today. As Director of the Information Security Oversight Office, one of my responsibilities is to oversee Government agency actions with respect to the National Industrial Security Program (NISP) in order to ensure compliance with established policy.

The overall framework for the NISP is set forth in Executive Order 12829, as amended (the Order). This Presidential directive recognizes the obvious imperative to ensure that classified information in the hands of industry is properly safeguarded. However, what is equally significant is its recognition that our industrial security program must also promote the economic and technological interests of the United States. As such, an essential element of the NISP is its acknowledgment that redundant, overlapping, or

unnecessary requirements imposed upon industry can imperil national security as readily as can the improper safeguarding of classified information. A common cause of unnecessary requirements is the inability of agencies to reciprocally honor a similar action taken by another agency, such as a personnel security investigation or a personnel security clearance involving the same individual – a practice commonly referred to as reciprocity.

Pursuant to the Order there are four signatories to the National Industrial Security Program: the Department of Defense (DoD), the Central Intelligence Agency (CIA), Department of Energy (DOE), and the Nuclear Regulatory Commission (NRC). In addition, all other Federal agencies that engage contractors on a classified basis are required to assume the status of User Agencies.

The Order assigns to the Secretary of Defense the responsibility to serve as the Executive Agent for the NISP. Furthermore, the Director of Central Intelligence (DCI) retains authority over access to intelligence sources and methods, including Sensitive Compartmented Information (SCI). Likewise, both the Secretary of Energy and the Chairman of the NRC retain authority over access to information under their respective programs classified under the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.).

In addition to overseeing Government agency actions to implement the Order, as ISOO Director, I serve as Chair of the National Industrial Security Program Policy Advisory Committee (NISPPAC), which is comprised of both Government and industry representatives. The NISPPAC advises me on all matters concerning the policies of the NISP, including recommending changes to those policies. The NISPPAC also serves as a forum for discussing policy issues in dispute.

Before the creation of the NISP in 1992, each agency had its own individual industrial security program. Each program had processes that were unique. The NISP has helped to create an atmosphere of cooperation for both Government and industry by eliminating many duplicative processes. More than ten years after its inception it would be hard to imagine an environment without the NISP. However, notwithstanding past successes, today's challenges require constant attention and effort from participating agencies in order for the NISP to achieve its full potential in promoting the economic and technological interests of our nation, especially recognizing industry's critical role in both the current war efforts as well as many of the "transformation" activities currently underway in much of the Federal Government. Inevitably, the leveraging of technology and services from the private sector are an integral part of these efforts.

Often, NISP participants refer to the program as a "partnership" between Government and industry. However, it is more than that - it is also a legally binding contractual relationship. As with all contracts, both parties commit to do certain things. Industry, of

course, agrees to protect classified information. The Government, in turn, agrees to do certain things as well. In fact, in many instances, Government action is a prerequisite for contractor action.

For example, contractors cannot provide an employee with access to classified information until the Government clears that individual. Yet, with respect to promoting our nation's economic and technological interests, agencies' inability to accomplish this and other prerequisites in a prompt manner or to honor reciprocally a similar action by another Government agency, has a significant and deleterious impact upon cleared industry's capability to support their Government customers.

Oftentimes, agencies cite fear of accepting an unknown potential security risk as the basis for not embracing reciprocity. I know of no empirical basis to support a claim that reciprocity reduces security or increases risk; instead, I contend that the failure to achieve full reciprocity can actually increase the overall security risk for the nation. First, needlessly requiring and reviewing security forms and investigative files, and oftentimes requesting duplicative investigations, all for individuals who have already been deemed trustworthy by another Government agency, needlessly distracts limited resources that can be devoted to the current unacceptable delays in processing new, initial clearance requests. Second, this practice has also contributed to a backlog in periodic reinvestigations. Ironically, the proven risk does not lie with individuals who transfer from Government to industry, industry to Government, or company to company and who

undergo the additional vetting process inherent to being interviewed and hired for a new job. Rather, the proven risk often rests with individuals who might be viewed as being in a “career rut.” Currently, such individuals are oftentimes experiencing prolonged delays in undergoing a periodic reinvestigation.

In addition, reluctance on the part of Government agencies to forego some "agency prerogatives" and fully embrace all the tenets of the NISP, especially reciprocity, hampers industry's ability to recruit and retain the best and the brightest in their disciplines as well as its capability to rapidly develop and field the latest technology when performing on classified contracts. As a result of this inability to achieve and maintain the NISP's full potential, contractors are hampered in putting forth the best conceivable efforts in both cost and capability in supporting their Government customers' needs. As such, the Government effectively ends up with less for more.

In order to assist in reducing clearance delays in industry, my office, through the NISPPAC, has served as a forum for industry to provide their concerns and recommendations to the Government's current working groups addressing personnel security clearances – specifically a group under the auspices of the National Security Council as well as a separate group under the auspices of the DCI's Special Security Center. Our goal is to assist in establishing an ongoing dialogue to ensure industry's unique circumstances are understood as Government agencies wrestle with the many longstanding issues that plague the personnel security arena – recognizing that overall

responsibility for personnel security policy is beyond the immediate purview of my office.

Even more immediate, we have recently initiated a renewed effort by the NISP signatories to implement near-term solutions to the issue of reciprocity within industry. The goal is to have NISPPAC issue and publicize a clear articulation of what reciprocity is (and is not) with enough specificity and substance that industry can hold Government agencies accountable for their actions in this area. I am pleased to report that we have succeeded in garnering senior level support for these efforts and anticipate formal promulgation within a matter of weeks. This declaration is not a silver bullet. However, it should allow contractors who experience failure on the part of a Government program or contract office to honor reciprocally a clearance action by another Government agency to seek immediate redress.

Many thousands of individuals within Government and industry are responsible for the progress made to date in implementing the NISP. There is more that needs to be done, and ISOO will be working closely with our partners in industry and Government in building upon a much needed renewed commitment to the NISP's original goals and objectives.

Again, I thank you for inviting me here today, Mr. Chairman, and I would be happy to answer any questions that you or the Committee might have.