**Testimony of**

# Doug Wagoner

## On behalf of the Security Clearance Reform Coalition

Before the Homeland Security and Government Affairs Committee
Of the U.S. Senate
May 17, 2007

Aerospace Industries Association
American Council of Engineering Companies
Armed Forces Communications & Electronics Association
Associated General Contractors of America
Association of Old Crows
Contract Services Association
Information Technology Association of America
Intelligence and National Security Alliance
National Defense Industrial Association
Professional Services Council










**SECURITY CLEARANCE REFORM COALITION**
**TESTIMONY BEFORE THE SENATE HOMELAND SECURITY AND GOVERNMENT AFFAIRS COMMITTEE**
**MAY 17, 2007**

Good morning Mr. Chairman and Members of the Committee. My name is Doug Wagoner and I am the Chief Operating Officer of Sentrillion. I am speaking to you today as a member of the Information Technology Association of America (ITAA) and I would like to thank you for this opportunity and for your continued commitment to reforming the clearance granting process.

For the last several years, ITAA has led the Security Clearance Reform Coalition[1] of ten trade associations seeking to bring industry perspective and recommendations to the clearance granting process. Several of our previous recommendations were adopted as part of the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA). Just as this series of hearings has sought to do, we hope to monitor the clearance granting process and make recommendations to both the Administration and the Congress to bring relief from the significant problems this dysfunctional process causes for industry. My comments today will focus on the process as it relates to collateral DoD clearance applications, but we believe that all of government would benefit from the adoption and implementation of these suggestions. It must be noted that industry does not experience the same delays for clearances in the Intelligence Community and, in fact, most of that community is currently processing clearances within the metrics established in the IRTPA.

As I am sure you are aware, industry continues to face significant problems with the clearance granting process that result in a negative impact to our ability to meet the national and

[1] The Security Clearance Reform Coalition is comprised of the Aerospace Industries Association, the American Council of Engineering Companies, the Armed Forces Communications & Electronics Association, the Associated General Contractors of America, the Association of Old Crows, the Contract Services Association, the Information Technology Association of America, the Intelligence and National Security Alliance and the National Defense Industrial Association and the Professional Services Council. We represent hundreds of companies that provide thousands of cleared personnel to the departments and agencies of the U.S. government.

homeland security missions of the United States. Delays in processing persist because of the government's failure to adopt 21st century technology innovations; agencies which continue to craft their own requirements for mutual recognition of clearances; as well as a lack of prioritization at some departments and agencies coupled with funding mechanisms that prevent investment in cost and time-saving technologies. Our assessment of the status of the clearance granting process would not match the rosy picture painted in the Administration report to Congress this past February, but would more closely resemble the General Accountability Office (GAO) (GAO-06-1070) report as an accurate picture of conditions in the process.

Industry views the clearance granting process as having four distinct parts and we have adopted the mantra, "One application, one investigation, one adjudication and one clearance" to simply express our goals for improving the clearance granting process. Unfortunately, we do not believe that any of these goals have been achieved. To help bring about change and provide options for consideration by both the Congress and the Administration, you will find attached as an addendum to this testimony our latest set of recommendations for improvements. I would like to highlight one recommendation from each of the four sections of the process and point to the improvements that its adoption would bring.

## APPLICATION

The single most critical improvement that *all* of government could adopt to improve the process would be the full and complete electronic application for a security clearance. As the stakeholders for the application stage of the process, collection and submission of the

completed application package is the responsibility of the agency or department that provides a clearance for industry personnel. There are three parts to an application – a completed form SF-86, a signed release form and a complete set of the applicants' fingerprints. Industry applicants for the Department of Defense (DoD) now use the electronic questionnaire for investigative purposes, or e-QIP, to capture the SF-86, but the other components of the application package are either not collected electronically at all or they are collected using such antiquated techniques and technologies that they are a burden to the system instead of an improvement to the process.

Fingerprints are still collected and submitted using paper and ink fingerprint cards and manual rolling of the prints. This is baffling to industry, as all armed services' recruits have their fingerprints collected digitally at recruitment centers, the Department of Homeland Security has adopted digital fingerprint collection technologies for port workers and much of the nation's local law enforcement now use digital fingerprint technology for criminals. Industry has even offered to provide the necessary technology to submit digital fingerprints, but this offer has been declined because the databases are, apparently, incapable of accepting such digital submissions. This prevents the fingerprint cards from being bundled electronically with the application and the signature and instead requires that they must be separately packaged and mailed for later marriage with the electronic SF-86. As you can imagine, this creates significant opportunity for fingerprint cards to be lost or delayed in transit. An all too often result of this condition is that e-QIP applications are rejected for investigation because the fingerprint cards are not received in a timely fashion.

Signatures for applications at DoD are now collected electronically, but they are collected by the use of a facsimile machine, rather than the widely available technology now found on most checkout counters in America. This technologically antiquated signature collection method has created such a drain on the system resources of DoD's Joint Personnel Adjudication System (JPAS) that they have posted an apology on their website to their users for the processing delays. Furthermore, it has created a new, extremely negative condition in the application process described as "out of synch" applications. "Out of synch" applications are applications that are submitted using the e-QIP electronic form SF-86 and appear to have been successfully submitted to JPAS. In reality, these "out of synch" applications are instead lost in the digital ether and are never received. Currently, there are estimated to be over 2,000 industry applications that are "out of synch" and, potentially thousands of applications from the armed services that have been lost in the same fashion. "Out of synch" applications are not discovered until there is such a delay in the receipt of an interim clearance for the applicant that a knowledgeable industry security officer follows up and discovers the loss.

Industry would like to congratulate and support the efforts of the new Director of the Defense Security Service, Kathy Watson, for identifying these and other problems and making the corresponding suggestions for improvements to JPAS to correct them. We have been disappointed, however, in the lack of funding and prioritization at DoD that has prevented their expeditious resolution.

Implementation of this critical recommendation can occur immediately if the Office of Personnel Management (OPM) would simply enforce its' published requirement that all

applications for investigation must be submitted electronically using e-QIP. This requirement was published almost two years ago, but OPM continues to receive and process between 25-40% of all applications in paper form. Large agencies, like the General Services Administration, also contribute to this problem by ignoring this requirement and requiring applicants to complete a paper copy of the 30-plus pages of the SF-86.

These inconsistent and disjointed application collection mechanisms that continue to rely upon manual submission of some or all of the components of the application create significant problems allowing the process to even get started. By eliminating any submission options except those using digital technologies, the application would be received, approved, and an investigation begun in a matter of minutes, instead of the weeks or even months inherent in the current process.

## INVESTIGATION

The primary stakeholder for the investigation stage of the clearance process for over 90% of all clearances granted by the United States government is the OPM Federal Investigative Services Division or FISD. FISD is responsible for verifying receipt of a completed application from the agencies and departments and initiating an investigation corresponding to the level of clearance that is being requested.

Here, too, the process would greatly benefit from the adoption of 21st century technology to eliminate the tremendous amount of "touch labor" involved in the processing of applications at OPM. For example, clearance applications - even those submitted electronically - are printed

out and a file folder much like one would encounter in a doctor's office with color-coded labels is created for each applicant. It is industry's opinion that it is this shuffling of the paper file, from clerks processing these files in the mine at Boyers, Pa., to the investigative personnel in the field and back again, and then finally on to the adjudicators that creates such a tremendous delay in the processing of clearances. Industry would recommend that government move to create and implement an end-to-end data management capability that begins with an electronic application created in e-QIP. During the investigative stage, that application would then be appended with relevant information obtained from commercial and government databases, such as credit histories and criminal records, and, finally, would be provided to the adjudicating agency as an interoperable electronic file with all relevant information readily available for adjudication. Instead, we currently have a process at FISD where electronically submitted information is printed out to create a hard-copy file, files are then mailed to investigators in the field for investigation, completed files are then tracked using manually affixed bar-coded labels and in many cases a hard copy summary is sent back to the originating agency for adjudication.

At the center of this tremendous amount of touch labor is the antiquated database dubbed PIPS or Personnel Investigations Processing System. This technology would have been abandoned and replaced decades ago in the private sector as out-of-date and a hindrance on efficiency. The system is completely isolated and does not share data directly with any other computer system in the application process. It would be impossible to make this system interoperable and to share data in real time in a cost efficient manner. Finally, the age of this system is prohibitive to the adoption and incorporation of most technological advances in

information management from at least the last decade. As long as OPM continues to rely upon PIPS, there will be no way to eliminate the tremendous amount of touch labor in the investigative process, nor will it be possible to provide data in an end-to-end paperless fashion for the efficient application, investigation and adjudication of clearance applications. This disability also adversely impacts on the implementation of the reciprocal acceptance of clearances.

A final note must be made regarding the sharing of data both to and from FISD. OPM has frequently pointed to the "imaging" of data, like fingerprint cards and completed investigative files, as "automation" of the process. To be clear, imaging is not automation and does not necessarily contribute in any way to the efficiency of the process, but is simply the digital capture of a picture of a document. Without additional technology to read the image and extract the relevant data, imaging does nothing to improve the process and instead creates another step that clearance applications must undergo for processing.

## ADJUDICATION

Accurate and reliable adjudicative outcomes can be improved through the receipt of complete cases from OPM to include full development and reporting of derogatory information in the course of the investigation. Currently, it is not unusual that, when relevant derogatory information is discovered, it is not fully explored, developed or mitigated in the investigative stage of the process, imposing enhanced and unnecessary risk assessment requirements on adjudicators. Some enhanced risk assessment requirements are necessary, for example in evaluating the trustworthiness of an applicant for translating services with ties or connections

to countries in the Middle East that are listed as state-sponsors of terrorism. But intentionally leaving issues undeveloped, or labeling applications as "closed pending," abrogates responsibility for completion of the investigation and only exacerbates the condition, making it harder for adjudicators to accurately assess an applicant. Of course, industry also feels that adjudication would be significantly enhanced and made more efficient with the adoption of the end-to-end data sharing capability mentioned above.

## RECIPROCITY

Bill Leonard at the Information Security Oversight Office and Clay Johnson at OMB should be applauded for their efforts to bring about the greater reciprocal acceptance of clearances across the federal government; but frequently their good intentions have been overcome by the intractability of old habits. This is in spite of the Congressional direction clearly provided in the IRTPA.

Trust in the adjudicative abilities of each agency, as well as the trustworthiness of the underlying investigative information used as the basis for the clearance, remains at the heart of the reciprocity issue. For example, empowering OPM as the single investigative source for the majority of the clearance needs of the government was a proper and correct step toward establishing uniformity and consistency in the process. Other steps, like the Central Intelligence Agency plan to enter unclassified clearance information into JPAS are applauded as enhancing the ability of agencies to verify clearances and should increase the trustworthiness of the data for users. But data sharing is still limited. While some agencies have indirect access to JPAS, as the sole system of record for collateral clearances for the

U.S. Government, all authorized agencies with a clearance granting mission should have direct and readily available access in order to give them the necessary tools to implement the reciprocity policies as intended.

Industry would ask Congress to reiterate and clarify their intentions included in the IRTPA regarding reciprocity to include the identification of agencies that are not in compliance with national reciprocity guidelines, and assign responsibility to compel those agencies to comply. Similar oversight should extend to the sharing of clearance data to verify the quality and completeness of clearance information being submitted to the existing clearance databases, namely JPAS and OPM's CVS. Without timely, accurate and reliable clearance information in a standardized, central database, reciprocity will continue to plague the clearance process with delays and unnecessary costs.

Industry would also ask Congress to clarify expectations regarding the implementation of Homeland Security Presidential Directive 12 (HSPD-12). HSPD-12 requires that all federal government employees and contractors accessing federal government facilities or information systems must be validated through a background investigation and issued an identification card attesting to the completion of such an investigation. Currently, it is not specified in law or regulation that the government is expected to accept as approved under the requirements of HSPD-12, without further need for investigation, all federal and contractor employees that currently hold a clearance. In order to prevent unnecessary and redundant investigations, and to reduce the workload on OPM FISD, as the identified entity responsible for investigations, we hope that this can be clarified.

## BUDGET

On one final note, Congress must provide innovative and flexible budgetary authority to create a reliable and sufficient funding source for these agencies to undertake these and other improvements necessary for a world-class, end-to-end clearance system that will be in compliance with the IRTPA by December 2009. FISD, for example, receives no direct appropriations and instead must pay for their operations through fees assessed on their customers. As such, the federal government must develop a more accurate system for estimating the demand of industry and government clearances, and the appropriate agencies should submit budget requests that mirror the anticipated demand, with a limited reliance on premium charges.

Mr. Chairman, it is our sincere hope that these recommendations provide options for improving the clearance granting process. It is, however, but a start towards a much-needed re-evaluation and re-engineering of how the security clearance community does business in the 21st Century. We are ready and willing to discuss all of the recommendations we make in the addendum and look forward to working with you and the Committee to bring about additional improvements to the security of the United States through improvements to the clearance granting process.

# Recommendations of the Security Clearance Reform Coalition For Improvements to the Clearance Granting Process

Presented to the Homeland Security and Government Affairs Committee
Of the U.S. Senate
May 17, 2007

Aerospace Industries Association
American Council of Engineering Companies
Armed Forces Communications & Electronics Association
Associated General Contractors of America
Association of Old Crows
Contract Services Association
Information Technology Association of America
Intelligence and National Security Alliance
National Defense Industrial Association
Professional Services Council

These recommendations are focused on the collateral DoD clearance granting process, since many of the IC agencies are running efficient processes using state of the art technologies.

These recommendations are based upon extensive interviews with the various stakeholders in the clearance granting process to better understand what happens to an application as it moves through the process and are bolstered by the numbers of clearances in the backlog, defined as non-compliant with the metrics of the 2004 Intelligence Reform and Terrorism Prevention Act. These numbers as of mid-February, when 459,598* cases were reported in process, are:

- Initial Secret/Confidential: 113,161 over 90 days old with 81,680 "closed pending"
- Initial Top Secret: 45,185 over 90 days old with 7,566 "closed pending"
- Top Secret Reinvestigations: 39,925 over 180 days old with 10,786 "closed pending"
- All Others (suitability, etc.): 41,372 over 90 days old with 12,906 "closed pending"

**TOTALS: 239,643 backlogged cases with 112,938 "closed pending" cases.* This amounts to 52% of all cases in process in the backlog and 48% of the backlogged cases categorized as "closed pending."**

***these totals DO NOT include secret/confidential reinvestigation numbers.***

## APPLICATIONS

1) End-to-End Capability: The process is one large paper shuffle and must adopt an end-to-end capability to share data interoperably in real-time. No such planning is currently underway, as there is no one manager for the process.

2) Require Electronic Applications: OPM must enforce the requirement published in the Federal Register requiring all new applications and renewals to be submitted via the Internet-based e-QIP. Currently, between 25-40% of all applications are still accepted in hard copy. Several major agencies, including the General Services Administration, still require applicants to complete paper applications and include other extraneous information, like resumes, as part of the application.

3) Clarify Metrics: Congress must clarify that the time frames established in the IRTPA for clearance processing begin when an application is actually received by the investigative agency, regardless of when it is actually scheduled. Frequently, the calendar for the investigation is not started until months after the application has been received by the investigative agency.

4) Improve JPAS: DoD must invest the funds necessary to make required improvements to JPAS. This is not happening at present and service is being degraded to the DoD adjudication facilities as well as to thousands of security managers in both government and industry who depend upon it for mission requirements. The JPAS user community and the Defense Security Service (DSS) have already identified the changes needed to

streamline and accelerate JPAS processing, but the level of priority for this problem seems to have fallen since last summer when DSS ran out of funding. These improvements include the ability to accept and capture digitized fingerprints and signatures from industry and eliminate delays and dropped applications caused by JPAS being out of synch.

## INVESTIGATIONS

1) Modernize Data Capture: OPM must modernize its data capture procedures. Imaging, while frequently cited as an "automation" of the clearance process, is nothing more than taking a picture of a document and is ineffective at capturing the data in the document for use in an information technology system.
    a. OPM must stop accepting fingerprint cards and start using digitized fingerprint capture tools such as LiveScan.
    b. Signatures on release forms can also be easily captured using technology at checkout counters across America and eliminates the need to print and mail release forms to investigators when needed.
    c. Investigative files are also selectively imaged, where using truly digitized information would allow for the preservation of the entire file, not just summaries, and preserve critical information like credit reports and criminal histories.

2) Modernize Data Management at OPM: OPM-FISD continues to rely upon PIPS, an antiquated stand-alone mainframe computer system that is not interoperable and cannot be made so. This reliance forces continuation of labor-intensive paper handling that significantly delays the processing of clearances. Many of the problems identified by industry in the process are related to or stem from this reliance upon PIPS.
    a. PIPS does case assignment, but once a case is assigned, it is printed out and mailed to investigators for processing.
    b. For paperwork management, OPM relies upon barcodes, which are manually keyed, printed and affixed to documents in the hard copy files.
    c. Only some of the information collected during an investigation is preserved for future review or access by the adjudicators and other critical information sources, such as criminal and credit histories, are not retained.
    d. CVS is an important tool, but cannot adequately verify a clearance since it relies upon batched data and is not real-time.
    e. OPM must begin to share investigative results electronically. Currently, they do not share any investigation results electronically, but they do image some results. This does not facilitate adjudication processes, as none of the data can populate data management systems at the adjudicating agency.

3) Eliminate the "Closed Pending" status for clearances at OPM: OPM categorizes investigations that are incomplete due to the lack of some data or incomplete status of some component of the application as "closed pending." Some of these incomplete files are then passed to the originating agency for adjudication, while other departments, like DoD, refuse to accept or adjudicate these applications in "closed pending" status. Since this information is frequently needed to make adjudicative risk assessments, agencies

are then forced to return the application to OPM, thereby incurring further charges to process the clearance.

4) Implement the Use of Phased Periodic Reinvestigations (PR): The federal government should direct implementation of phased periodic reinvestigation (currently being implemented only by DoD) to realize the full benefits of scaling the PR in such a way that limits the use of costly and time consuming field investigation. Using commercial and government databases, cleared personnel are evaluated for any activity that would require further investigation (Phase I). If the Phase I results (automated checks and selected interviews) are favorable, there is no need to proceed to the costly field investigation (Phase II). Phased PR's can be conducted more frequently with less cost, so that the cleared personnel – those most in a position to cause harm to the United States – are more effectively monitored. It is conservatively estimated that such an approach could save 20% or more of the cost of conducting periodic reinvestigations.

5) Implement ACES or the Automated Continuing Evaluation System: ACES, by automatically checking a variety of government and commercial databases, can almost constantly monitor the activities of cleared personnel, daily checking them against government and commercial information sources for any activity that could require further investigation. This would facilitate and accelerate the government's ability to properly manage and monitor current clearance holders and to identify significant problems and issues of security concern whenever they occur, rather than on a periodic term (every 5-10 years). Any cases where issues are identified through ACES would undergo a full periodic reinvestigation. This approach would not only enhance security at a reasonable cost but would quickly provide a huge baseline of data to evaluate.

## ADJUDICATIONS

1) Adequately Develop Derogatory Information: OPM has modified the criteria to which clearances at various levels are investigated, including dropping efforts to investigate and develop derogatory information for Secret collateral clearances. Such a change in the process makes it difficult if not impossible to effectively adjudicate many applications.

2) Enhance Training Standards: Develop and implement standardized professional training and certification criteria for adjudicators across the federal government. This would create equity in the training and development of adjudication officers and improve reciprocity of clearances by building trustworthiness across federal agencies with the application of adjudicative standards.

3) Establish Common Recordkeeping: Establish and implement a common approach across all agencies, using existing central clearance databases like CVS, JPAS, and Scattered Castles, for the recording of waivers, conditions, and deviations in order for adjudicators and security officers to have access to this information when taking an action to reciprocally accept another agency's clearance or access determination.

## RECIPROCITY

1) Increase Clearance Data Sharing: Intelligence Community agencies should be required to populate JPAS with clearance/access information on non-classified employees. All such data should be validated to ensure that it is not corrupting critical, accurate information about existing clearance holders contained in the databases.

2) Reinforce Uniformity in the Application of Reciprocity: Some Intelligence Community agencies are requiring that a clearance must be "active" rather than "current" before it will be considered for acceptance under reciprocity rules. This approach necessitates obtaining the prior investigative file and re-adjudicating the clearance. This is a costly, time consuming and unnecessary process under existing policy and is in violation of the spirit, if not the letter, of the IRTPA. It is also in direct conflict with the provisions of EO 12968 and OMB memoranda of December 2005 and July 2006 (Checklist of Permitted Exceptions to Reciprocity) which require a valid "access eligibility determination."

3) Provide Access to JPAS for Authorized Agencies: All authorized Federal agencies should be given direct access to JPAS, as the sole system of record of the U.S. Government for all clearance and access eligibility determinations, in order to more fully and efficiently realize the goal of clearance/access reciprocity.

## BUDGET AND PERSONNEL

1) Establish Efficient Budgetary Mechanisms: Budget issues were partly to blame for the processing moratorium on industry security clearances. As such, security clearance reform must include budget improvements as well. For instance, the federal government must develop a more accurate system for estimating the demand of industry clearances, and the appropriate agencies should submit budget requests that mirror the anticipated demand, with a limited reliance on charged premiums.

2) Enhance OPM Workforce Capabilities: Likewise, OPM's workforce capabilities must also be aligned to meet the anticipated demand for security clearances, as well as the demand for investigations of government and contractor personnel under HSPD-12 (industry estimates this requirement to include over 10M individuals). While some flexibility currently exists, industry is skeptical that it can meet these anticipated demands.

3) Build More Accountability Into the Invoicing Process for Clearances: OPM should not collect fees from the agency until the background check is completed and should provide greater clarity in their billing practices per the DoD IG investigation of these practices.