

HSPD-12 Rebadging at JPL: a Historic Primer from Employee Perspective.
(I am not a lawyer, but very much prefer rule of law to the alternatives)

U.S. is attacked by a bunch of hacks with box cutters.

President forms "Homeland Security" bureaucracy and issues a number (20 as of now) of directives addressing perceived vulnerabilities.

HSPD-12 is one of the shortest, shorter than HSPD-4 that gave us the rainbow of threat colors.

The only connection to the threat of terrorism in HSPD-12 is in this sentence: "Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated."²

HSPD-12 says "'Secure and reliable forms of identification" for purposes of this directive means identification that ... is issued based on sound criteria for verifying an individual employee's identity". There no mention of any checks other than ID verification.

In the HSPD, Department of Commerce (and its component NIST) was charged with writing an implementation standard. FIPS-201 is this standard.

Within the executive branch, the office charged with investigating employees is, quite reasonably, Office of Personnel Management. It plays the role of HR for Federal government. OPM had an established set of procedures for handling hiring for Civil Service positions. To avoid duplication of effort, identity verification and suitability determination functions were combined.

NIST, limited by time pressure to use the existing processes, identified NACI (national agency check with written inquiries) as the minimum investigation level acceptable for badging (because it was the minimum investigation level acceptable for federal civil service employment). There are a few obvious problems with this approach. First, there

² In logic this construct is known as Association Fallacy, and it is aided by omitting commas delineating the location clause:

- Federal Facilities have varied IDs
- Some Federal Facilities are attractive targets
- "...terrorist attacks need to be eliminated"
- Therefore ID problem need to be solved

Other examples of this fallacy include "'Imagine a world in which Saddam Hussein was there, stirring up even more trouble in a part of the world that had so much resentment, so much hatred that three ... that people came and killed three thousand of our citizens" and "If we're successful in Iraq... we will have struck a major blow right at the heart of the base, if you will, the geographic base of the terrorists who have had us under assault now for many years, but most especially on 9/11."

are many people working for government subcontractors for whom NACI is meaningless. Recently transplanted foreign nationals will not have sufficient history in the U.S.; their employment, education and, criminal history (if any) is inaccessible to U.S. investigators³. Foreign nationals are typically not admitted into civil service. Second, there was no prior requirement for contractors to undergo “suitability” determination (other than NAC, with criminal history check), unless they were in “staff-like” positions.

Here is the logic of the first potential legal issue:

1. Presidential Directive, while binding on Executive Branch, cannot override U.S. law.
2. HSPD itself does not call for collection of information related to suitability and not needed for positive ID
3. Privacy Act of 1974 does not allow Agencies to collect information not required by statute or Executive order⁴
4. Yet contractors are required to undergo “suitability” determination based on OPM extensive investigative questionnaires (SF85 itself and forms sent to references go as far as soliciting feedback on drug/alcohol use, mental and emotional stability, trustworthiness and financial integrity)

The way some agencies handled this legal issue is by indicating clearly that the new burden of suitability determination is unrelated to the badge issuance.⁵ Others, notably Department of Energy (DOE), issued an agency order limited the re-badging only to those who would be required to go through the suitability investigations anyway (e.g. civil servants and contractors with security clearances). DOE allows employees of national labs (Federally Funded Research and Development Centers, like JPL) to continue with the existing, local badges.

NASA, with JPL as its only FFRDC, and possibly not knowing of DOE FFRDC status, did not distinguish between us and other centers.

³ Notably, there is still no guidance on how foreign national badging will be handled (unless such guidance is provided by NASA, JPL indicated that it will continue using current badging procedures for these individuals, which would probably drive Lou Dobbs insane). GAO flagged this issue as a problem in a February 2006 report, “ELECTRONIC GOVERNMENT: Agencies Face Challenges in Implementing New Federal Employee Identification Standard”,

⁴ The Privacy Act of 1974: *Each agency that maintains a system of records shall-- (1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President;*

and

the term "maintain" includes maintain, collect, use or disseminate;

⁵ For example, NOAA document, “Homeland Security Presidential Directive HSPD-12 PIV-1 Implementation And Suitability Processing” states that “The suitability background investigative process and the issuance of the PIV Credential process are two very distinct processes”. Agency contracting officer has full discretion as for applying “suitability” criteria to contractors.

Because the directive originates with the Executive, it can only apply to the Executive branch entities⁶. Only executive agencies, such as NASA, can conduct investigations and authorize badge issuance. Because entities outside of Executive branch cannot be compelled to participate in the issuing process, they cannot possibly be identified as legitimate recipients of any information derived from the investigation.⁷

NASA interim directive (NID to NPR 1600.1) takes this into account by requiring that anyone accessing the submitted information and the results of the investigation be a civil servant. Contractor organizations are specifically denied access to any developed derogatory information.

NASA does not have the funds allocated to implement the rebadging and is required to absorb the costs from the existing budget. Similarly, NASA provided JPL with neither funds nor workforce to implement the directive (other than the costs paid by NASA to OPM for the investigations).

In the current JPL implementation, the personnel (contractors hired by JPL) who access OPM information (to verify the completeness of the information submitted) do so on behalf of JPL, and report to JPL office of protective services. JPL security personnel, and possibly others at JPL have access to the forms. This is contrary to the letter of the NID, a probable violation of the Privacy Act by NASA, and an unnecessary liability for JPL and Caltech when things will inevitably go wrong. Further, JPL has instructed (albeit mildly) group supervisors to coordinate their negative feedback with HR/ER.

FIPS-201 requires a process in place for handling appeals. JPL still has none.

All throughout the process was driven by artificially-imposed deadlines and prioritizing schedule over privacy and security. A number of obvious loopholes and unresolved issues are still very much evident, and probably will not go away. To iterate and expand:

1. Investigations are not required for temporary employees with residence under 180 days
2. Investigations cannot be done on recent immigrants and those living “off the grid”
3. As of July 25, with over half of the lab initiated for processing, no specific “suitability” criteria or appeal process are defined
4. There is still no clear process for those who decide not to undergo the investigation and the checks. Some personal information (including SSN) is submitted by JPL/contractors “case workers” to OPM to initiate the process without prior consent by the employee, even if they do not intend to stay at JPL.

An ideal solution would be the DOE approach. Absent that, any implementation should address privacy and fairness; the process should be defined in sufficient detail and communicated openly, and should be fully in accord with JPL core values.

⁶ other than, possibly, the Office of Vice President

⁷ Privacy Act of 1974: *No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains...*