Defining User Attributes
For
Authority-Based Access Control

Written by:
K. Krasnow Waterman
Patricia K. Hammar

For

Department of Homeland Security
HSHQDC-06-C-00110

Through

May 15, 2007

Table of Contents

List of Tables

List of Figures

Executive Summary

Throughout the government, agencies are working towards the technical ability to quickly share the right information with the right people. Rather than disseminating digital "publications," these projects are seeking ways to allow individual users to reach across disparate systems and get the specific information they need and have the authority to receive. Significant efforts are being made to architect an Information Sharing Environment that will make it possible to appropriately and securely share terrorism, law enforcement, and homeland security information both across the agencies of the federal government and more broadly with state, local, tribal, foreign, and private partners. Also underway are parallel efforts such as the National Health Information Network, linking government health and emergency management functions with private hospitals, clinics, and individual physicians. Academia and private industry are addressing similar pressures to let individuals discretely access information from a wide variety of sources with whom they have relationships.

One piece of the challenge is how any system will "know" which people to give which access. Traditionally, this has been done by maintaining lists of people, authorized users, by name. History has taught us that this is not an optimal method because it requires significant effort to keep the lists up-to-date and in synch. Or, more often, minimal resources are deployed towards keeping the lists accurate and many individuals retain access long after they should not, which poses a real and sometimes disastrous security risk. Another approach to access control is to focus on "what" people are instead of "who" they are. In other words, what attributes do we need to know about a person to determine whether they are authorized to access a system or a specially protected subset of information in a system? Some examples of attributes are the name of the person's employer, their employment status, which clearances they hold, and/or the purpose for which the person is seeking the information.

Policy advocates and technologists alike agree that the way to provide attribute information to a system is not to aggregate all attribute data or take control over other organization's systems. A preferred method would be to call dynamically "authoritative sources" – repositories of regularly updated, relevant information that already exist for other purposes – each time a person seeks access, in order to determine from the best information available *at that moment* whether the individual should receive access. For example, if access is restricted to people who work for a particular organization, we could find out if they are an employee by asking that organization's human resources system. This will be much more effective and efficient than needing to update and synchronize a list of names.

This project is a first step towards identifying attributes needed for such a concept to work. Our hypothesis was that working with attributes in this way would be practical and economically viable only if we could define a small number of tractable, highly reusable attributes that could provide the needed information to most authority-based access control systems.

In this initial project, we identified attributes that were most often sought by the broad range of systems in our experience. We sought ways to generalize them so that a small number could be used by the largest number of systems. We developed a vocabulary and framework for describing them. We sorted them into two categories, those that can and should be handled first, due to primacy and availability and those which offer lesser benefits across the community as a whole or present technology or policy challenges. Then, we investigated the rules for access to four DHS systems, deconstructed them to identify the required attributes they implied, and mapped them to our attribute model. Where possible, we identified the specific value(s) a system would need to receive to grant access and included multiple equivalents of that value when such would be expected from disparate sources. When available, we identified the "authoritative source," the system from which the attribute information could be drawn, and the field name within it. From this activity, we were able to identify those attributes which are likely to be used by the most systems and additional issues which will need to be addressed.

This work is cognizant, but independent, of any particular design for a rule-based access control system. For example, in one instance the potential data requestor may need to withhold some attributes and only transmit those that are needed by a system's rules (i.e., a federal employee would not reveal security clearances to a foreign government's unclassified system). In other cases, data may require such tight security that even its access criteria cannot be revealed and each requestor must put forth all his attributes for consideration; this might apply to Secret Service data on the travel of the President. In these, or any other designs, if there is an access control rules engine, there must be user attribute information to reason over. This project focuses on what those attributes are and how many are in common. Once known, they may be delivered to any rule-based access control system.

Our work appears to provide support for a breakthrough for access control in the government's highly distributed environment. Many have argued for a more robust, more consistent security methodology than a UserID and password backed only by a static user list. But, there is broad concern about the complexity needed and the ability of smaller organizations to participate. We believe that we have shown that the ability to dynamically call a very few attributes – there are only 13 "primary" attributes in our model – will fulfill the underlying needs of most access control rules within the federal government and between the federal government and its partners; these attributes are sufficiently basic that they are likely to be available even in very small partner organizations. Beyond that, we have identified only six additional attributes which would further enhance the granularity of access grants or extend the availability of dynamic access control to systems with more unique requirements. We strongly recommend continued work, gathering additional access rules and mapping additional systems, to refine the attribute list and to begin proof of concept access control systems.

1) Background

Department of Homeland Security Secretary Michael Chertoff has repeatedly stated that sharing information is a critical goal of the Department. This is consistent with the recommendations of the 9/11 Commission;[1] orders of the President,[2] recent acts of Congress;[3] and public demand.[4] The Secretary wishes to *"ensure that information is gathered from all relevant field operations and other parts of the intelligence community; analyzed with a mission-oriented focus; informative to senior decision-makers; and disseminated to the appropriate federal, state, local, and private sector partners."*[5] To achieve this ambitious goal, individuals and organizations will need to adopt new ways of thinking and working; the shift from "need to know" to "need to share" is underway. Technology, too, must be ready and in place to support the shift.

In the current technical environment, it can be quite daunting to meet the Secretary's goal

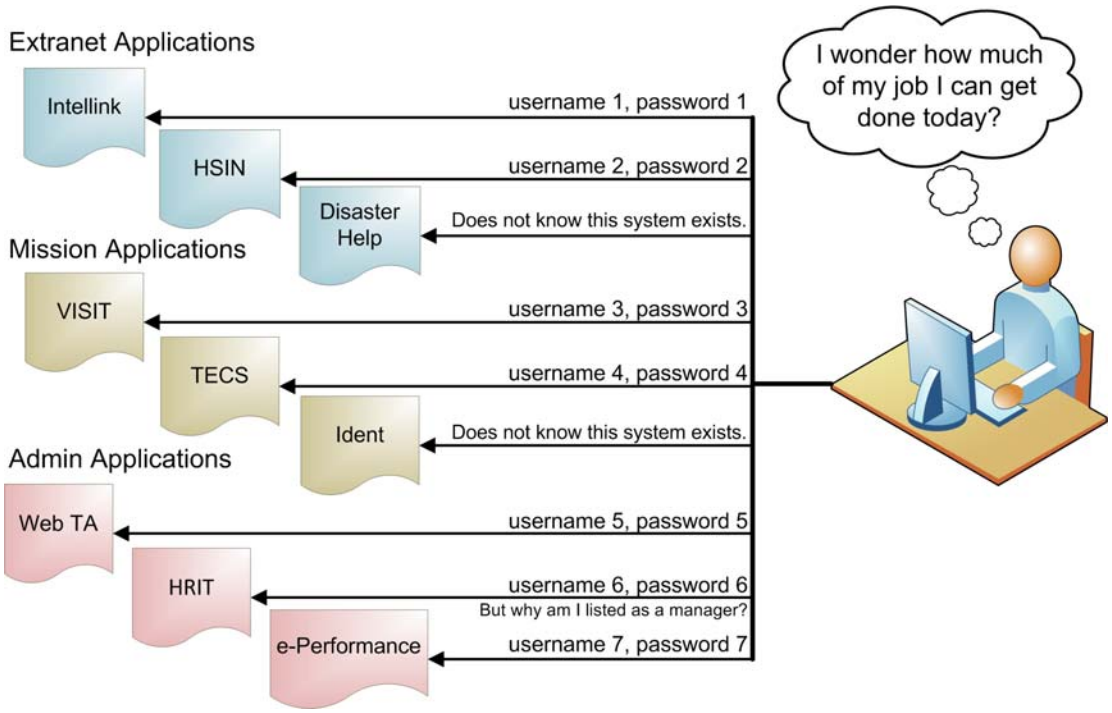


Figure 1 Current Process

---

[1]

[2] See, e.g., Executive Orders 13356 and the superseding 13388, requiring agencies to establish an "information sharing environment" to facilitate the movement of terrorism, homeland security, and law enforcement information.

[3] See, e.g., Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, creating a legislative mandate for the information sharing environment.

[4] See, e.g., the three reports of the Markle Foundation on National Security in the Information Age, recommending the creation of a SHARE network to facilitate information flow.

[5] Excerpted from Sec. Chertoff's Six Point Agenda (7/13/05).

of gathering all the relevant information to address a particular issue. One needs to get permission and establish user accounts on many systems. Often those systems are not available through the same computer device and workers need to go to different rooms or even different buildings. There are a number of "single sign-on" projects underway,[6] seeking to provide users a single gateway that would gather relevant user information and pass it to any systems from which they seek information. This design would make it possible to federate queries across multiple systems at one time, a tremendous efficiency advantage for the users.

Current system-by-system access controls present a number of problems beyond user inconvenience. These systems require manual administration of authorized user accounts on a by-name basis, often without current, high quality information about the users. Such manual administration is costly and that cost is multiplied by the number of discrete systems using their own credentialing efforts. They can't leverage more recent "strong-authentication" credentials. These systems generally don't support "fine grained" access controls which would make it possible to limit access to users with appropriate "authorized purposes" and they won't scale to include direct access for all appropriate users. Because they are independent of one another, they tend to apply inconsistent access policies, even within the Department. With so many known limitations to the quality of the security, system business owners have strong incentives to limit data access as the primary means of reducing risk and cost. This is not unique to the Department or the federal government. It is a vestige of how computing systems were designed and been built over time.

In 2005, Kim Cameron, a Microsoft architect, led a public and professional dialog on what is needed to begin to address that and other related problems. He authored seven "Laws of Identity" to define an "identity metasystem" for the Internet. Like the government and its partners, web-based and web-using entities do not share system architectures or access rules, nor do they have common definitions for individuals or the relationships which make it appropriate for them to receive information. Cameron and his colleagues recommended the creation of an identity layer for the Internet "to provide a reliable way to establish who is connecting to what." This is the government's problem as well, though it might be expanded to say "to provide a reliable way to establish who *should be* connecting to what."

Equally relevant to the government context, his second "law", "Minimal Disclosure for a Constrained Use", recommends that the least possible identifying information about an

[6] The Department of Homeland Security (DHS) is engaged in a single sign-on pilot funded by the Information Sharing Environment Program Manager with the Department of Justice and the Institute for Intergovernmental Research (an organization that provides information exchange for state and local law enforcement). In that pilot, users will obtain single sign-on access to data in law enforcement systems from each participant: TECS (DHS), ICAV (DHS), JABS (DOJ), and RISS (IIR). And, the Department is cooperating with a Global Justice initiative, called Global Federated Identity and Privilege Management (GFIPM) and led by the Georgia Tech Research Institute, to define needed sign-on metadata for the state and local law enforcement community to work with the federal law enforcement community.

individual be passed to a system in order to support the claims that the individual is entitled to access the information sought. We agree that users are often asked for far more information than is needed to determine whether access is appropriate. This occurs for a variety of reasons. To save time, access request forms and scripts are often reused even if the access rules do not require the same information. Equally often, access rules such as legal and policy constraints, are not well relayed to system administrators. And, if each person in the chain of development adds one additional piece of requested user information on the "we might need it later" or "as long as we're asking" theories, the total collection can be much greater than needed.

Another current access control problem is that often users are vetted and granted access by a person who knows them or knows the person recommending them. This "personal trust" system cannot scale as the volume or dispersion of potentially appropriate users grows. Equally important, as the number of interacting systems and relevant rules grows, humans cannot remember them all or compute the priorities and overlaps of the many applicable access rules. Conversely, electronic systems can consistently apply the rules regardless of size and scale. Designed properly, systems also can identify when rules clash or overlap.

In order to proceed with such a concept, the identities of users must be presentable in a consistent manner that can be understood by such systems. "Consistent" in this context does not mean "identical," but rather sharing framework concepts sufficiently that relevant information can be accepted or translated into something acceptable. Looking forward, the next goal will be to eliminate the manually administered lists because they are difficult to keep current and synchronized with other organization information. For example, if an appropriate supervisor tells a system administrator to give John Q. Doe a user account on a system, the administrator often has no means of knowing quickly when Mr. Doe has changed duties or terminated employment. Sometimes, the person who provided the credential remembers to report those changes to the system administrator and sometimes not. Often, terminated employees' accounts only are removed during periodic sweeps through the account lists.

A substantially improved method will be to have the user's credentials checked electronically each time he requests access to information. This will require that systems be able to immediately acquire all attributes about a user necessary to determine if the user does or does not meet the requirements of an access rule. In this context, an

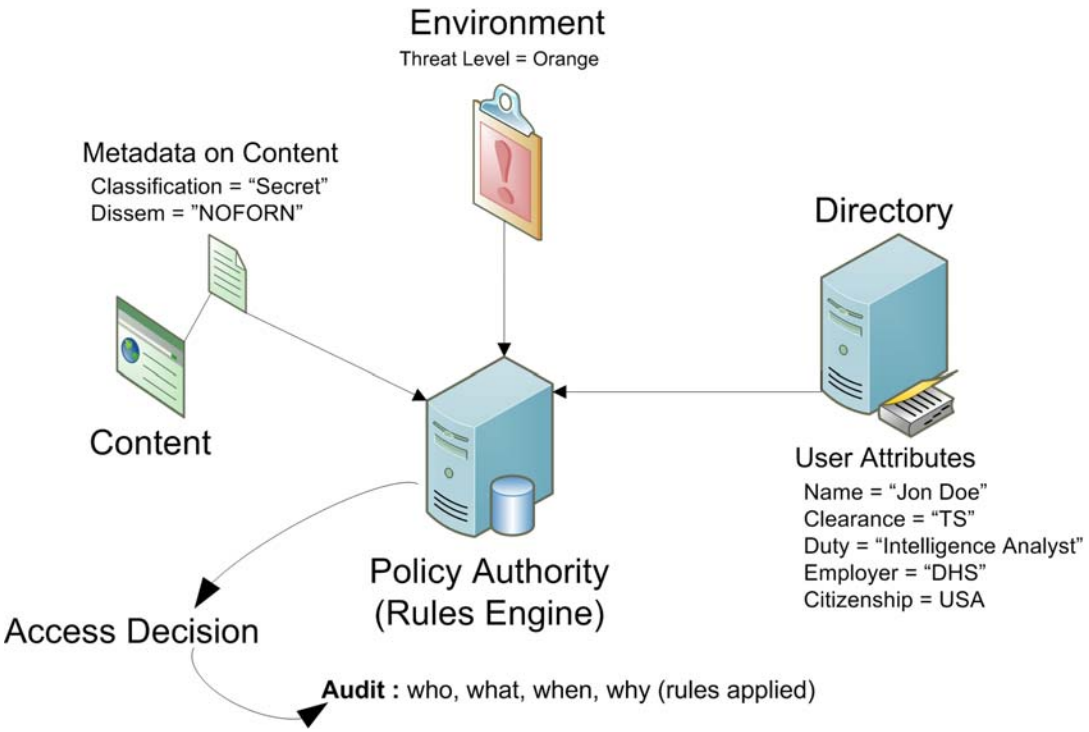


Figure 2 Authority Based Access

"Attribute" is any fact known about a person. Relevant attributes for achieving access control will be information about job duties, clearances, citizenship, etc. For attribute information to be reliable it must come directly from an "authoritative source." For full automation to occur, the authoritative source must be another data system.

Current information systems often control access through a set of "roles"[7] which, in general, simply mirror positions within an organization. Access rights are grouped by role name, and the use of resources is restricted to individuals in that associated role. For example, within a hospital system the role of doctor can include authorizations to perform diagnosis, prescribe medication, and order laboratory tests; and the role of researcher can be limited to gathering anonymous clinical information for studies.[8]

"Role based access" is evolving towards "rule based access" to account for the reality that access is granted for specific reasons, which sometimes do not align with job titles. Business conditions (i.e., understaffing) and environmental conditions (i.e., disaster), result in dynamic reallocation of responsibilities and alter the correct response to a request for information. Persons serving as "duty agent" for the day may need to access different information from what they do on the days in their regular assignment. A person in Toledo could be assigned to assist with a matter in Tucson, if it were easy enough to get them shared access to the electronic files. And, 9/11 showed that many people should have had access to information which was previously considered irrelevant

[7] For additional information on Role based access, the authors recommend http://csrc.nist.gov/rbac/
[8] "**An Introduction to Role Based Access Control**" NIST CSL Bulletin on RBAC (December, 1995)

or inappropriate. In each of these cases, the important question is not "what is your job title?" but rather "do you meet the criteria for access to this information at this moment?"

Our discussion here looks at the foundational attributes that current access rules imply. The goal is to break down the many rules and roles into their component parts, to discover the attributes upon which trust decisions are made. In the long term, attributes may be aggregated into "roles," which are not job titles, but instead descriptions of groups of people with common information needs, such as "supervisors in DHS," "all DHS intelligence personnel," and "all of John Smith's direct reports." As capabilities become more sophisticated, so too will the roles, permitting groups such as "lawyers in General Counsel, except the one under investigation," "private sector and local law enforcement in a threatened area," and "State law enforcement officers working on case number xxx."

The most complex of these "roles" actually incorporate an additional factor: context.(i.e., a "law enforcement officer seeking a fugitive" rather than a "law enforcement officer"). As a practical matter, current technology limits us to knowing what a person is permitted to do (i.e., "law enforcement officer authorized to seek fugitives") rather than what they are actually doing (i.e., "Officer Smith is approaching the door of Mr. Doe"). For this reason, we address these more complex descriptions still as "roles." As technology and skill to handle context-based criteria improve, it is anticipated that security access rules can be made more or less restrictive based upon the dynamic factors, such as the general threat environment (i.e., more restrictive in times of low threat and less restrictive during crisis or vice versa).

It is important not to fall into the trap of trying to predefine all of the possible roles that might be access triggers. It would be impractical, probably impossible, to try to identify the thousands of roles that people use as the talisman of authority to access information. The numbers are even greater if changing business practices and priorities are taken into account. It will be much more effective, and more readily achievable, to understand the factors which combine to make a role and to permit each data steward to combine the factors in any way appropriate to his mandates.

Being able to identify the specifically needed user attributes and authoritative sources will provide a significant step on the path to digital implementation of Departmental and federal information sharing policy. It will support the development of the Information Sharing Environment. A system that can electronically pull current user attributes and match them against current access rules, will ensure more consistent application of policy and law; reduce reliance on personal trust, and increase reliance on institutional trust. It will reduce human error and reduce manual workloads while increasing the total volume of information access requests which can be handled. Such a system will radically increase the speed with which new partners can be given proper access permissions; reducing the months of negotiating written access agreements to milliseconds of computer processing. And, a system handling this level of detail can provide more meaningful audits and performance metrics. It will ensure that more people get the right information at the right time.

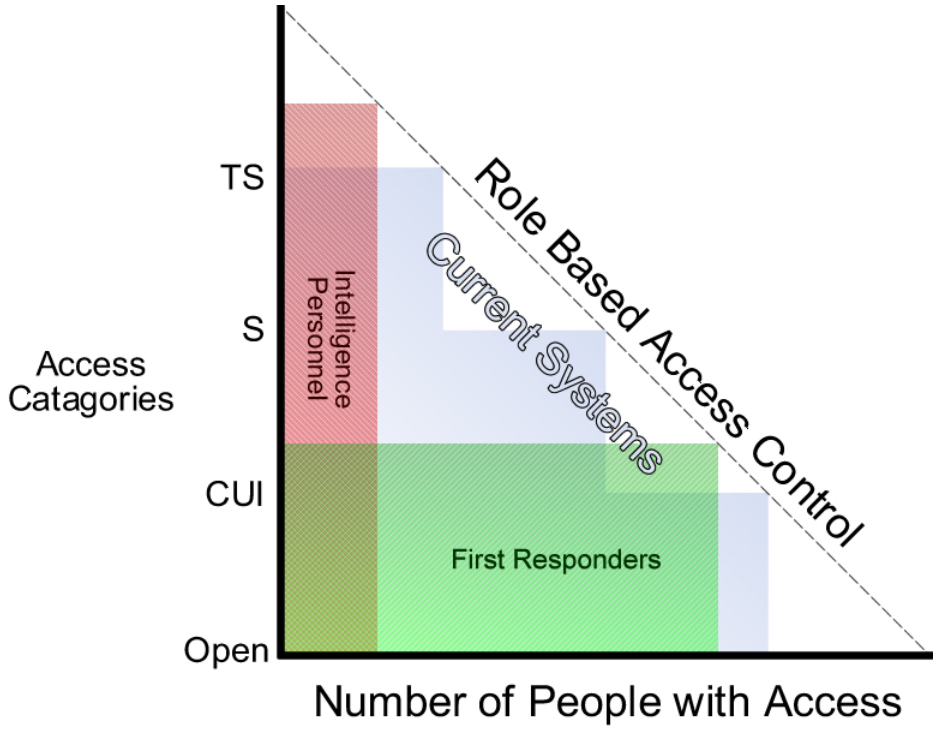


Figure 3 Missed Opportunities for Information Sharing

The figure above, shows graphically how the current stepped system – one that treats everyone as either in our out of a broad block of information – leaves gaps in what information can get to individuals authorized to see the information. As we increase the number of attributes upon which access decisions can be made, we increase the number of appropriate people who can have access, ultimately getting all the information to all the people authorized to see it at the right time.

This report addresses the first effort to determine which user attributes would be needed to fuel common system access rules and what authoritative sources are available currently to provide the information. This initial project looked at four systems, intentionally from an array of business operations within the Department. Two were related to internal administration: ePerformance, the employee performance evaluation record system, and T&A, the time and attendance system. Two provide DHS information and information exchange capabilities to state and local workers as well as DHS employees: DHelp, the Disaster Management Help portal, and HSIN[9], the Homeland Security Information Network.

[9] There are a large number of HSIN Communities of Interest (COIs) that self govern the vetting process. Four of these COIs were reviewed: Law Enforcement, State and local Intelligence, Pandemic Influenza and Coast Guard.

2) Scope

Since an attribute is simply a fact about an individual, there are an infinite number of attributes about any given individual. These attributes, however, are not all used to make decisions concerning an individual's access to data. In this report, we have limited ourselves to those attributes about an individual that are used to make information access decisions. This section outlines four ways that attributes are used for access control decisions in systems, one which is within the scope of our paper and three others which are not. These are Authentication, Security, Authority, and Preference attributes. They respond to the following questions:

- Authentication: Are you the person you claim to be?
- Security: Are you coming to my system in a sufficiently secure way?
- Authority: Should you have access to the information, or some of the information, in my system?
- Preference: How would you like to see the information?

As described below, Authority attributes are the only ones within the scope of this paper.

a. Authentication Attributes: Outside Scope

Some attributes are used are for Authentication, which is the process of ensuring that a user is the person represented. These attributes can represent knowledge, such as high school attended and city of birth, or physical manifestations, such as hair and eye color. They can be changeable, such as passwords and weight, or can be generally immutable, such as fingerprints and height. Attributes used strictly for authentication are outside the scope of this study.

However, sometimes, authentication attributes are considered in information access decisions. For example, although a fingerprint record is not an attribute upon which access decisions are made, a fingerprint used for authentication could be passed to a criminal database to confirm that the user had no criminal record and that fact might be the basis upon which an information access decision is made. In this case, the real information access attribute is that the person has no criminal record and the authentication of the user in this example is used as a proxy for this attribute.

b. Security Attributes: Outside Scope

Another set of attributes, Security Attributes, describe the means by which an individual accesses data. These are attributes that describe the level of protections or safety measures used to access the system. An example would be that more data may be available to an individual that accesses the system through a Virtual Private Network or Secure Socket Layer than an unrestricted internet connection. More information may be made available to an individual on a JWICS terminal than a person entering a system through their commercial mobile phone. Or, more information may be made available to a person providing a fingerprint rather than a password. Security attributes are not

discussed in this paper because they are not about the individual's authority to get a certain piece of data but rather about the system's level of trust of their means of access. In those cases, the system is attempting to limit the likelihood of leakage to a non-authorized user.

c. Authority Attributes: In Scope

The only attributes that we are addressing in this paper are those attributes that the system uses to make decisions as to an individual's permission to see data. We will call these Authority Attributes. They define "what" a user "may" access. The level of assurance that the system has in these attributes is critical. For each attribute, an authoritative source must be identified from which the data can be accessed by the system. The quality of these authoritative sources will impact a data steward's decision of whether to accept the attribute as a criterion for granting access.

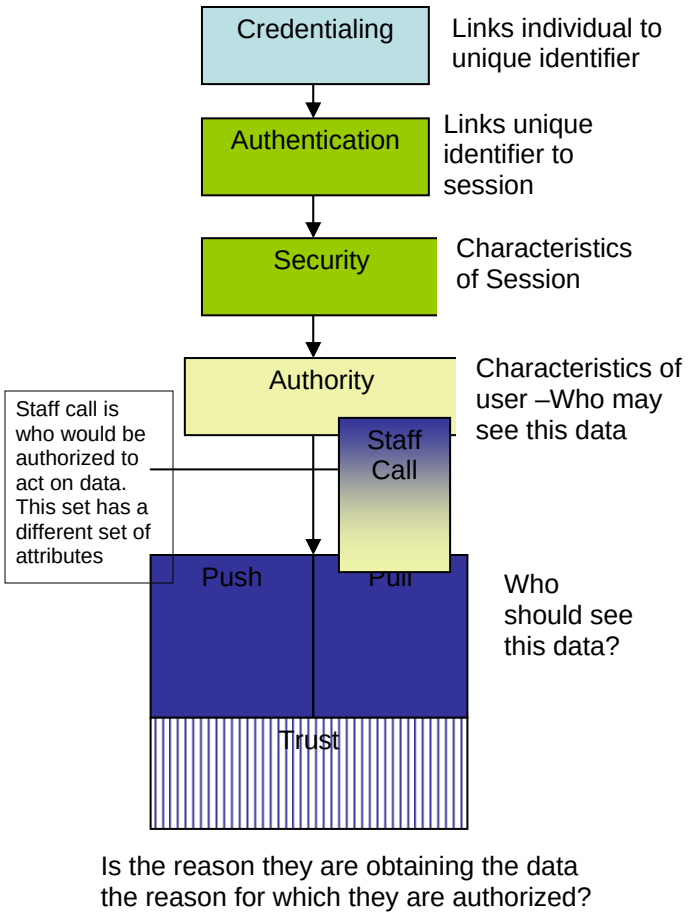


Figure 4 Attribute Types

d. Preference Attributes: Outside Scope

There is another set of attributes that do not require authoritative sources, these attributes identify user preferences. Preference Attributes can be used to differentiate between various types of information that you are authorized to see. If an individual is authorized to see all personnel files but chooses to look at only certain files, the system need not evaluate the choice. If an individual is authorized to see all terrorism data within a given classification but chooses to only look at terrorism data about nuclear incidents, or within a given time frame, they are choices that can be made exclusively by the user, without external input or reasoning. Preference attributes are outside the scope of this paper because they do not require data custodian permissions.

e. Attribute Disambiguation

Sometimes, it is not readily apparent which sort of attribute a particular piece of information represents. For example, consider the question: who is capable of doing a certain task (has certain skills)? This question parallels the information access question and can fall into either the Authority or Preference attribute groups. If it is a skill that requires confirmation, such as surgeon, and an authoritative source would be required prior to relying on the attribute, it should be designated as an Authority attribute. If, on the other hand, it reflects a willingness, such as willingness to work overtime or to travel, it should be tagged as a Preference Attribute. Some skills might possibly be in both categories, such as language skills. Rarely, language skill could be an Authority Attribute; there may be a circumstance in which capability to speak a language must be validated before providing documents or allowing access to witnesses. But, most often the ability to speak a language is reflected in an expression of a Preference Attribute; a user prefers to only receive information in a language he speaks.

f. Authorized Purpose v. Action

The last issue pertaining to scope is the proper use of authority. This paper is limited to the task of determining if an individual has a valid and authorized reason to access information. This paper does not address the active management of trusted users; it does not seek to identify the means to ensure that they are only using the information for their valid and authorized reason. As an example, if a state police officer has access to NCIC data in order to perform his job, we are not looking at controls that would ensure he not also use that access to check on his daughter's new boyfriend, which is an unauthorized use.

Table 1Attributes

Decision-Maker	Attributes Sought	Indicia	Project Scope
System Owner	Authentication	Biometrics, unique identifiers	Out of Scope
Security Administrator	Security	.mil, .gov, mobile, JWICS terminal	Out of Scope
Data Steward	Authority	Job role, location	In Scope
User	Preference	Options selected	Out of Scope
Security Administrator	Trust	Audit logs	Out of Scope

3) Investigation Methodology

The investigation methodology approached the gathering of Authority Attributes from both current operational and policy perspectives. This is important, because it is sometime difficult for people to put a large number of policies into practice, and policies sometimes do not dovetail with practical realities. To standardize the attributes at the core of access policies, we must recognize and address any inaccuracies or variance in interpretation in policy implementation.

The investigation collected system access rules, legal access rules, system structure, and the business demographics of the users. The collected information was then analyzed to determine which of the information sought from a potential user was an authority attribute.

a. Data Collection

Optimally, for each of the systems investigated, effort should be made to gain a 360 degree view of the access rules. That is, the goal should be to understand the rules for access to the information in the system from the perspectives of all the people connected to it, whether the owner, administrator, or user. The primary parties and perspectives identified appear below:

Table 2 Data Collection

System Information	Source: Business Owner and…
Existing system rules	System Administrator
Existing source for accessing and vetting attribute information	System Administrator
Existing system data dictionary	System Administrator
Privacy Act documents – Privacy Impact Assessment System of Records Notice Routine Use Notice	Office of the Privacy Officer
Federal Information Security Management Act report	System Administrator/ Information Security
e-Authentication work for the system	System Administrator
Other laws or regulations that restrict access to information in the system	Office of the General Counsel
Information Sharing Access Agreements	Office of the

(MOUs, treaties, contracts, etc) with restrictions on access	General Counsel
Policies and informal rules	Users
Current user demographics	System Administrator

Over the course of the project, a Data Collection Worksheet Packet was developed to ensure that future work in this area can be conducted consistently and efficiently. A copy of the Packet is included at Appendix A.

i. System Access Rules

Understanding what rules drive access control in existing systems is a critical factor. These provide the minimum threshold for gaining any access to a system and the rules for tiers of access, where such functionality exists.

Early in the development of business systems, access rules were often not written down, and a system administrator simply accepted user names from someone they trusted, a "gatekeeper". Even that process had *implied* rules. For example, if the gatekeeper left the organization, the system administrator looked to that person's replacement or business unit for gate keeping. The gatekeeper, too, was using some rules, whether subjective – "I only grant access to people I know personally and trust" – or objective – "I only grant access to people in law enforcement jobs who work narcotics cases."

Today, system designers work with business owners of systems to more clearly define access rules. Together, they lay out the parameters for the people who can have access. For each system we examined, we requested copies of any system design documents that addressed such requirements and the points of contact that provided the criteria. We also asked for data dictionaries that would show specific data elements used for permissioning.

ii. Legal Access Rules

There are many kinds of data that are regulated by law. For example, laws provide limitations on the right or method to access records about individuals, their health, finances, and electronic communications. Perhaps the best known is the Privacy Act, which for most situations doesn't define these rules, but provides a framework for each agency to establish the rules of access for data in its custody. Under that law, agencies must identify 1) which data may be accessed, 2) by which categories of person, and 3) for what purposes; the latter two criteria will provide significant insight into user attributes an automated system would need to be able to access. We sought to find all such laws, regulations for each system. While others are aware of some of the laws, the best source for such information are lawyers assigned to the business owner by the Office of General Counsel.

iii. Technology Policy Access Rules

There are no known government-wide technology policy access rules that address authority. Technology policy in this general area includes the Federal Information Security Management Act (FISMA) and the related NIST implementation documents, the Government-wide, GSA led e-Authentication program, the credentialing efforts such as FIPS 201 based on HSPD-12.

FISMA prescribes the level of system protection warranted by the level of risk to the data. FISMA solely addresses compliance with system software and hardware security standards for access (i.e., intrusion) and does not consider the risks associated with the access decisions themselves. As the following figure shows, the rules addressed in this paper are the policy rules implemented by the access control portion of a system. FISMA is more focused on whether an unauthorized user can tunnel into the system or piggyback on an authorized user.

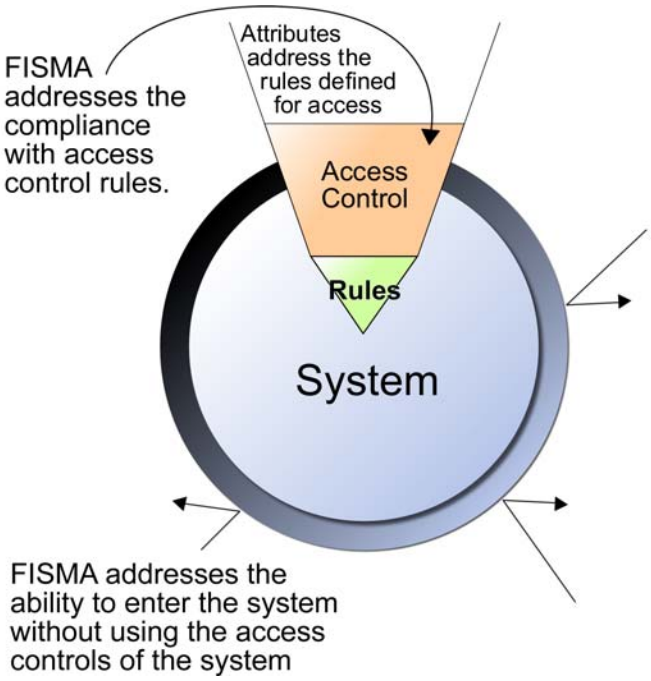


Figure 5 FISMA vs Access Authority

Electronic authentication[10] (E-Authentication) is the process of establishing confidence in user identities electronically presented to an information system. E-Authentication establishes that the person attempting to use a given unique identifier is the person the system expects them to be. In response to HSPD 12, the NIST Computer Security Division initiated Federal Information Processing Standard (FIPS) 201, entitled *Personal Identity Verification of Federal Employees and Contractors*, for improving the identification and authentication of Federal employees and contractors for access to

[10] http://csrc.nist.gov/pki/BioandEAuth/

Federal facilities and information systems. These address Authentication Attributes, which are outside the scope of this report.

iv. User Access Rules

Often, the number and complexity of access rules are unknown to individual users. Yet, they too are gatekeepers for the data in systems. People ask them directly for information contained in a system to which they have access. If asked, many people are unaware of the informal rule sets they've created for such situations. However, careful questioning can uncover them. It is important for users to understand that there are no right or wrong answers; they must be encouraged to describe when they have (or would) give or refuse to give information. Also, where possible, information should be elicited to determine when the user would seek permission from a third party and what role that person has. We developed an interview methodology to do so and applied it with users for each system.

v. Existing User Base

Understanding the user base provides important insights. System owners often estimate usage at much higher numbers than supported by system administration statistics. Gathering information about the size and demographics of the user base, to the extent possible, make it possible to determine whether the expected population, or which segments of the population, are actually using the system. Establishing the difference between optimal user base and current user base will support projections and calculations of performance metrics.

b. Analysis

Before data collection began, a list of probable attribute classes was prepared, based upon experience in other work. As system material was gathered, the attributes required by them was mapped to the draft master list. Based upon challenges in mapping, the master list, the concepts, and/or definitions were modified. Significant analytic challenges are described below.

The variation in how attributes are currently collected sometimes complicates the underlying relationship between the attributes. An example is work location which may be tracked in many ways, such as building code within an agency, address, zip code, geo-code or region. At first glance, these look different and in some cases are difficult to "translate" one from another. As we examined this and other issues, we see that they may all be answers to the work location question. It is important in these instances to ensure that this is the attribute being answered, that there are not multiple issues contained in one piece of data (as an example building number within an agency could simply be used to track location or could be organizationally significant as well if the

locations also represent work units). In the end, establishing semantic standardization could allow much less "translation", calculations and other actions to allow the use of current data in other systems.

i. Ontology

While analyzing user attributes, it is readily apparent that they can be organized in an ontology. For example, they can be organized into attribute ***properties, sub-properties***, and ***values***. If Person is a Class, then Employer is a Property, and Employer Type is a Sub-Property. The varied examples of things that fit into each of these properties would be called Values. For example, "FBI" and "Microsoft" are both possible values for the property Employer. And, in the context of this paper, "federal government" and "private industry" are possible variables for the sub-property Employer Type. This is described generally as "Person has an Employer: Value" and a specific instance might be "Bob Q. Doe has an Employer: FBI and has an Employer Type: federal government"

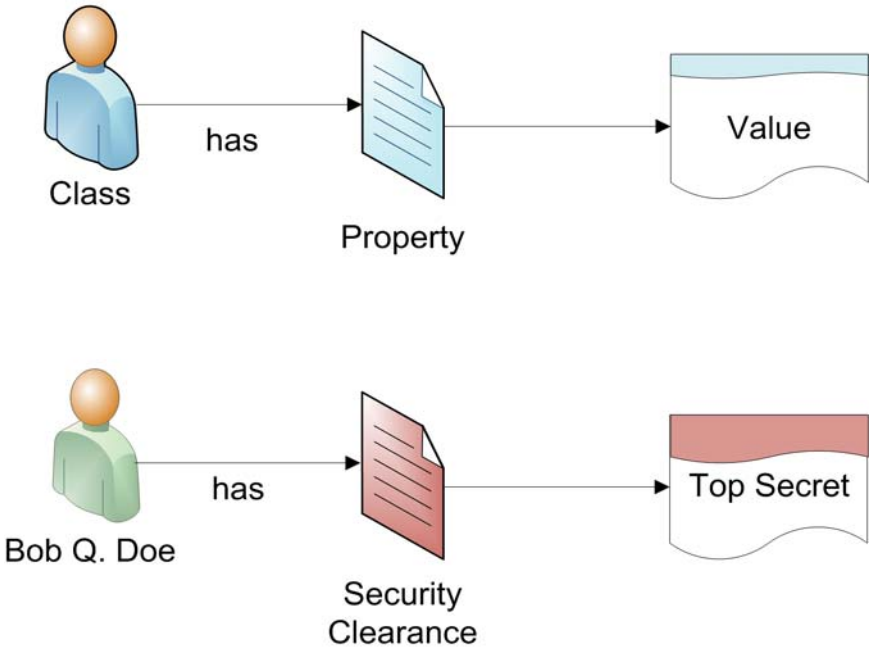


Figure 6 Ontological Relationships

As described in the Scope section, these properties can be clustered together into attribute groups such as Authentication Attributes and Authority Attributes. We chose not to describe those clusters as formal properties. Although this is the ontology we use in this paper, the specific ontology we describe is not critical to our analysis. To stress this point, we will map the structure to one or more existing or proposed ontologies. The primary message is that the framework is readily structured as an ontology and can be represented in the multiple ontology structures used by entities that will participate in the Information Sharing Environment.

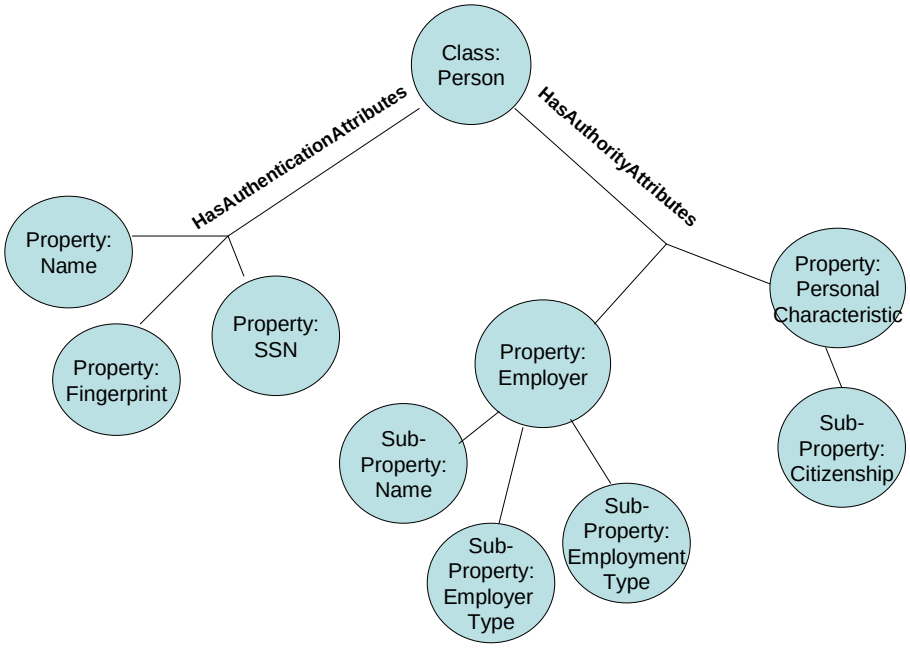


Figure 7 Ontology

In building access rule ontologies, though, we recommend that significant attention be paid to whether an item can be considered a value rather than a property, whether multiple items can be clustered into a more broadly described property.. We note that it is easy to rapidly expand the number of attribute properties by seeing each value as representative of a distinct property. For example, in an early draft, whether someone was in the Senior Executive Service was considered an attribute, but later it was determined that this information could be a "value" of the sub-property "management level." This is important because the smaller the number of total attributes; the more practical and manageable the system will be to implement.

ii. Taxonomy

Many of the needed attribute values are part of hierarchies, and knowledge of those structures will be necessary to make access decisions. For example, federal government access to information about US citizens is regulated by the Privacy Act. One requirement under that law is that information only be used in ways compatible with the purpose for which it was collected. 5 USC Section 552a(a)(7).[11] That means that the access rule will need to know what "authorized purpose" ("mission") values are included within the originally stated purpose.

[11] The law contains many requirements and multiple exceptions which are not described here. An excellent discussion of the Privacy Act and decision flow diagram were prepared by SRA (A. Slomovik) for the Information Sharing and Collaboration Office

Imagine that we had only this one Privacy Act rule and the taxonomy below. According to the taxonomy below, if information was collected for the purpose of criminal law enforcement, access could be given to a person with "authorized purpose" attribute values within the taxonomic hierarchy: "Law Enforcement: Criminal: White Collar," "Law Enforcement: Criminal: Drugs," or "Law Enforcement: Criminal: Violent." That same information could not be given to individuals outside the hierarchy, for instance with "authorized purpose" attribute values of "Law Enforcement: Civil: Child Support" or "Diplomacy: Immigration."[12]

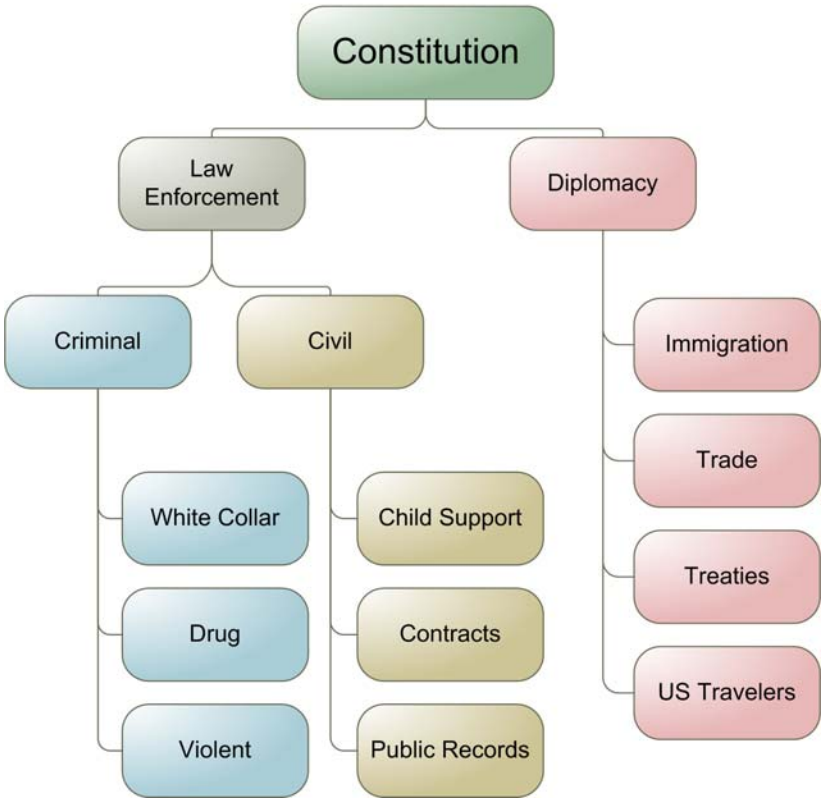


Figure 8 Sample Basis of Authorized Purpose

Attention must be paid to where attribute values are likely to be hierarchical and, to the extent practicable, such determinations should be described in the attribute descriptions.

[12] If Customs and Border Patrol had gathered information about cross-border drug dealers in a system of criminal case files, under this Privacy Act rule a Department of Justice Civil Division attorney working on child support matters could not access the files to try to determine if a particular parent might have hidden assets. And, a Department of State employee could not determine if someone who had applied for a visa was a criminal suspect. This does not mean the taxonomy or rule are wrong, only that there are other rules that also impact these decisions.

iii. Relationship

Most user attributes are meaningful in context, based upon their relationship to other attributes. For example, holding a security clearance alone is not sufficient reason to be given access to information. In order to gain access, an individual must *both* possess the necessary clearance *and* be engaged in an activity to which the information could reasonably be related. Because these two attributes must be delivered together, the ontology must ultimately reflect that relationship.

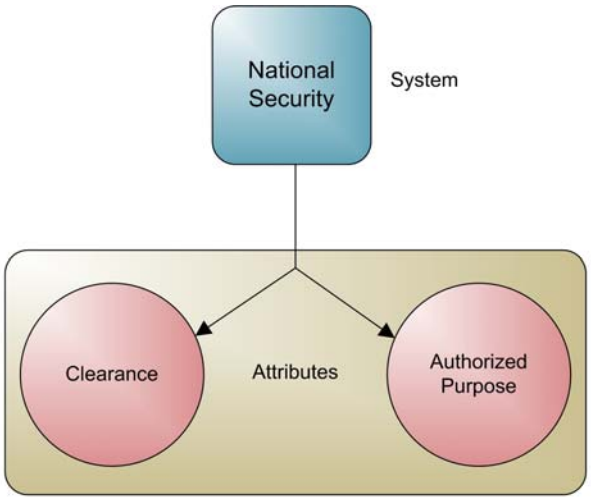


Figure 9 Relationship between clearance and authorized purpose

In a completely different vein, it may be equally important to know the relationship between the attribute Employer" and the attribute Employment Type. Two individuals who have "DHS" as an attribute value of Employer may not get the same access to information if one has an Employment Type attribute value of "permanent" and the other has "contractor."

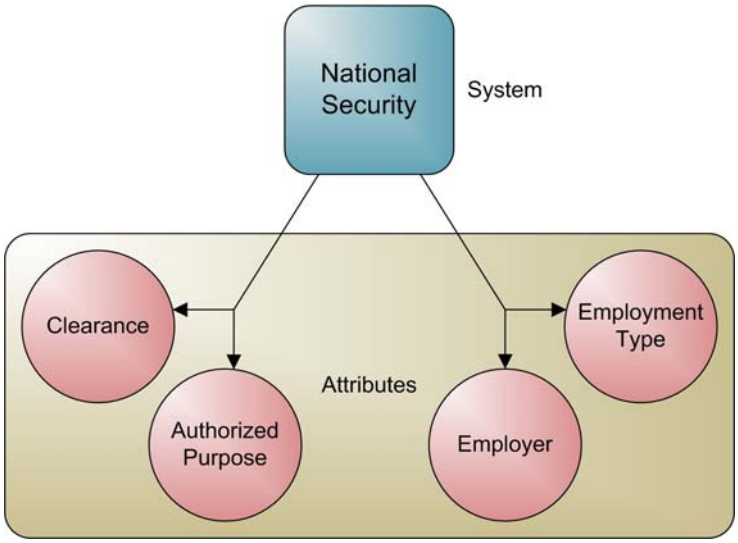


Figure 10 Relationship between attributes

As attributes were collected and mapped, analytic attention was paid to these relationships, which are discussed in the attributes section as well.

iv. Proxy

In this project, "proxy" means any attribute value that is used to imply another term, phrase, or attribute. A simple example is that all FBI employees hold Top Secret clearances, so knowing a person has the attribute of employment at the FBI means knowing they hold a TS clearance. A more complex example arises from the use of the term "sworn."

In the law enforcement community, the attribute "sworn" is often used to determine whether a person can or cannot have access to a system or particular information. Usually, the term refers to "sworn law enforcement officers." What is that a proxy for, what is the decisional criterion? Careful analysis reveals that "sworn" is not a term used consistently as a proxy for one attribute.

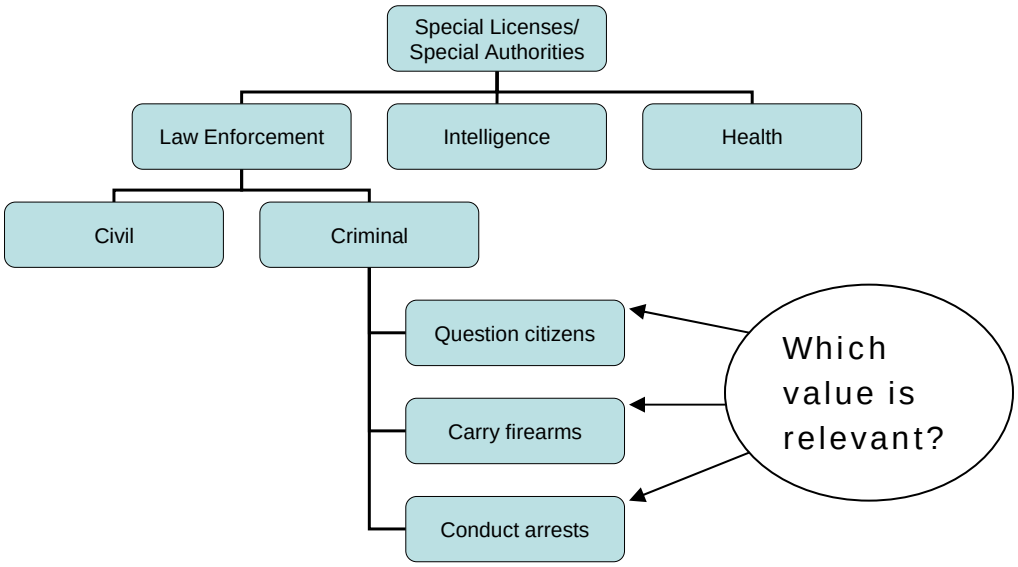
Although the word "sworn" is the short-hand form, whether someone has sworn an oath is not the seminal question. Many people are required to take an oath to enter their profession (i.e., lawyers) or begin their employment (i.e., Georgia Tech employees[13]), but the law enforcement community wouldn't give them access to law enforcement systems just because they swore an oath to someone. In many circumstances, being "sworn" also

[13] See, Loyalty Oath in the Hiring Packet of Georgia Institute of Technology (http://www.ohr.gatech.edu/departmental%20folders/employment_web/forms/hiringpacket-affiliate.pdf).

signifies authorized to carry a gun but, again, information isn't provided to them because they have the power to shoot someone. "Sworns" have the authority to investigate crime, to make an arrest, and to request prosecution. In some jurisdictions, other people hold some of these authorities as well: analysts may investigate crimes and prosecutors can have the power to arrest. Some systems allow these other persons access to the system or information. Thus, while "sworn" is a proxy to each party, it isn't the same proxy across parties. By parsing their authority to this level of detail, we are able to inquire which sub-authority is the decisional criterion.

Some proxies are much less obvious than others. On example of a less obvious proxy is the grant of a supervisor's permission. Since the supervisor will not necessarily be known to another agency's business owner, the approval must represent some other meaning. Perhaps it is the proxy for an authoritative source, confirming an assertion by the requestor that his agency's systems can't yet confirm. Another example comes from the ePerformance system when it pulls information about an employee's "Pay Table." While the name of the table is normally used to identify the group of possible salaries an individual can earn, it has a much less obvious meaning. The field "PAY-TABLE-CODE" provides information only when OPM authorizes a special rate,[14] that is when the government can't effectively recruit or retain individuals with a specific skill or expertise. It's likely to indicate that someone is an Information Technology specialist, or a chemist, or a nurse. So, these pay table names may be proxies for a portion of "authorized purpose" information.

Figure 11 Proxy values for "Sworn"



[14] Pursuant to 5 USC § 5305.

v. Calculated Attributes

Often, people cannot obtain the information they need directly from authoritative sources. To address this problem, they often create complex attributes or attributes that truly are a conglomeration of other attributes. In the semantics of this paper, these are Calculated attributes. Following the math analogy, calculated attributes are like most numbers, they are always the product of underlying prime numbers. Calculated attributes are identified in the Attribute Map with labels such as CALCULATED FROM or CALCULATED BY, followed by an explanation of the underlying attributes used to produce the calculation. This allows us to minimize the number of attributes that we need to track and allow the access systems, in the long-term, to accomplish the calculation.

As an example, the ePerformance system makes heavy use of calculated values. For example, it uses occupational series, grade, supervisory codes and working titles to figure out if an individual is a supervisor or manager, a person who should have the authority to evaluate the performance of others.

vi. Equivalents

An equivalent is something which means the same thing but is called by a different name by different groups. For example, "lstnm," "lst nm," and "last name" are equivalents. It is anticipated that different systems will have equivalent field names and values which will need to be accepted through the use of translation tables. Equivalents are different from proxies because, to the extent necessary, they have the same meaning where proxies imply, or can be used to derive, other meanings.

vii. Disjuncts

An important concept necessary to building an efficient structure for user attributes is the ability to accept disjunctive values. This means that the values for one property can be entirely unrelated to each other. For example, the Special Authorities property could be satisfied by such diverse values as "carry weapon," "prescribe narcotics," or "provide legal representation to employee sued in individual capacity." Though this may seem illogical at first reading, it will work because the access control system will pick out the value it needs and disregard the rest.

4) Optimal Attributes & Priorities

a. Optimal attributes

This study appears to confirm that, if defined properly, the total number of Authority Attribute properties that are likely to be consistently called for by systems should be a relatively small number. The working theory is that most government systems could successfully manage access control with less than twenty well-defined attribute

properties. Not that every system would call each attribute property, but that this aggregate number should be able to service the majority of requests.

Optimism about the small number of properties arose during the study when it became clear that some early considered attributes could be categorized as "values" of larger attribute properties. In an early draft, whether someone was in the Senior Executive Service was considered an attribute, but later it was determined that this information would be a "value" of the "management level." "Law enforcement" is a value of an "authorized purpose" or "mission." "Sworn law enforcement" is a value of "special authority" or "special license" and, since it has multiple meanings, should probably be more correctly identified as "authority to conduct a criminal investigation" or "arrest power."

b. Priorities

It was anticipated that systems used for very different purposes would share a number of attributes. We knew that most systems would need to know a user's employer, employment status, and legally authorized purpose for acting (e.g., law enforcement, intelligence, human resources administration). And, we suspected there would be a relatively small constellation of attributes that would overlap across systems and make up the majority of needed attributes. Our investigation confirmed that the following attributes are the most often needed and the most cost effective authoritative sources for them.

i. User Identity – Authentication Attribute

Table 3 User Identity

Attribute	Explanation	Example(s)	Common Source	Maximum # Values / User
Unique identifier	Linking mechanism to attributes	Name, Fingerprint, Hash code, SSN, Employee ID #, RSA Token Signature, Digital signature, Issuer Identification, PIV	HR system, E-Authentication	1
Pseudonym	Any other name used by or applied to an individual	Name before/after divorce, Nickname, Consistent error		Multiple
Birth date	When linked to name reduces likely individuals to nearly one	12/12/1967	HR system	One

a. Unique Identifier

The unique identity of an individual user is rarely, if ever, needed to determine whether that individual meets the criteria of a system's access control rules. However, the unique identifier will be needed to capture all of that individual's relevant attributes (used like a primary key, which links all relevant tables in a database structure), to search in the authoritative source systems for that person's information and to be sure that person is distinguishable from anyone else with a similar or same name. In addition, most systems will require the unique identifier for audit purposes (e.g., to find out "who was that Texas law enforcement officer working drug crimes who accessed our system?").

Some of these are more available than others. The attribute values, which are infrequently used to determine access, include signatures, digital signatures and those unique identifiers assigned to an individual by an individual system or program, such as the serial number or bar-coded information on an agency's proximity swipe card.

Another Unique Identifier ultimately may overtake all others. In August 2004, the White House issued Homeland Security Presidential Directive 12, Policy for Common Identification Standard for Federal Employees and Contractors. Under that direction, the National Institute of Standards and Technology (NIST) has issued instructions, commonly known as "FIPS 201",[15] for the creation of a common badging standard. The Personal Identity Verification (PIV) standard is intended to effectively bind an individual to his identity. Because the standard is required of private companies providing contract services to the government, and they will in turn require it of parties providing related services to them, it is expected that the use of the standards will spread widely within the United States.

FIPS 201 addresses many authorization issues, to obtain a badge, certain procedures must be met. These procedures, and the process by which they are correctly giving a badge to the person that the badge is for, is not an issue we are addressing. The fact that the person has a FIPS 201 badge may be used as a proxy for other attributes and as they become more prevalent a FIPS 201badge could be used as a unique identifier.

b. Pseudonym

Many people are known or have been known by more than one name. Most commonly, women add or subtract last names upon marriage and divorce. Many people have nicknames used so pervasively that they appear in official systems. And, some, like one of the authors of this paper, has a name which others so consistently find difficult that variations of the name are persistent. The author, for example, uses a name in the format FirstInitial MiddleName LastName. However, many government systems are structured only to accept FirstName MiddleInitial LastName, so others routinely enter her nickname

[15] "Personal Identity Verification (PIV) of Federal Employees and Contractor," Federal Information Processing Standard 201 (http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf).

or middle name in the first name field. This is also a significant issue for people who have more than three names, which is the norm in large segments of the world's population.

c. Birth Date

In the absence of better identifiers, a birth date is often linked with a name, which narrows the field to one or a small number. While there may be many people sharing common names like John R. Smith, very few will share the same birth date in the same year. Occasionally, there are multiples but this form of near-unique identification is the best available information in some non-federal entities.

ii. Highest Priority Attributes

Highest priority was assigned to attributes for one of three reasons: the attribute is sought frequently; the attribute is readily available from authoritative sources; and/or the attribute can reasonably be represented in a numerical form and aggregated. Frequency is a true test of priority; the ability to collect most-often-sought attributes will provide the fastest path to usability. The second and third criteria were applied to address current limitations and are the *caveats* to referring to this group as exclusively the "universal core". If certain attribute information is not readily available, then the ability to deliver functionality will be delayed. And, numeric representation is a requirement due to the limitations of most available software products in the area; although expected in the future, the products generally are not yet able to accept many values per user.

The following chart shows the full set of primary attributes.

User Primary Attributes for
Federal Government Authority Access Control

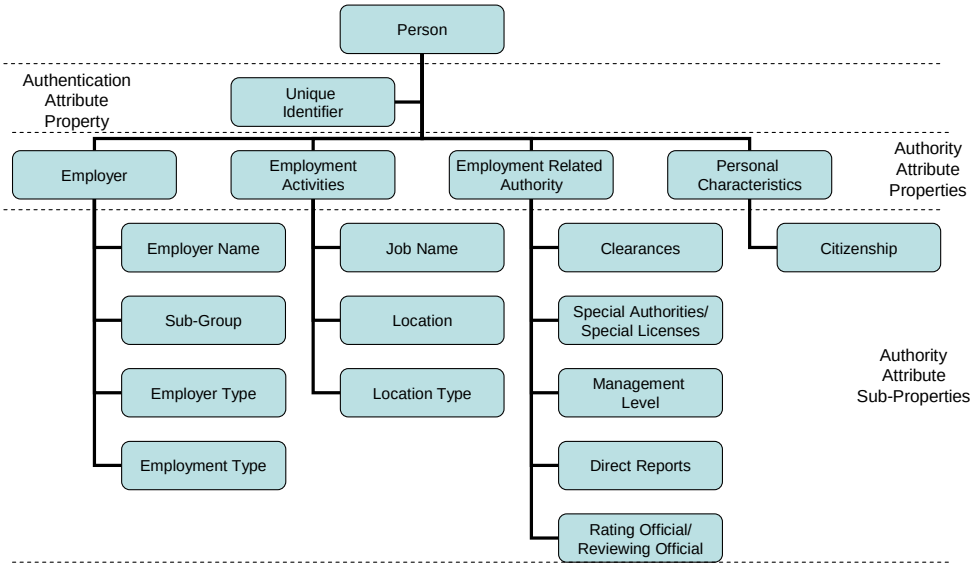


Figure 12 User Primary Attributes

1. Employer

Table 4 Employer

Attribute	Explanation	Example(s)	Common Source	Maximum # Values / User
Employer Name	Proxy for list of possible authorized purposes.	DHS employee = "immigration administration" or "law enforcement" but not "tax collection"	HR system, OPM, Agency finance system (for contractors)	Multiple – Multiple jobs
Employer Subgroup	Narrows proxy list of possible authorized purposes	I&A = intelligence, ICE/Gangs = "law enforcement" sub-purpose = violent crime"; "drugs"; "organized crime"	HR system	Multiple
Employer Type	Establishes relationship of organization to the federal government	State government, local government, Private industry, Foreign government		1
Employment Type	Establishes relationship of individual to the	Permanent, Temporary, Detail,	HR system, Agency finance system (for	Multiple

	federal government	Contract	contractors)	

a. Employer Name

Information about a person's employer can provide information critical to an access decision. Typically, knowing the name of the employer is equivalent to knowing something about the work a person might be doing, the mission he might be serving.[16] If the employer is a government entity, this single fact usually provides the finite list of authorized purposes of any of its employees. For example, if a person works for the FBI, he could have an attribute value of "law enforcement: criminal" or "intelligence: foreign counterintelligence" or "administration of government: human resources" but would not have a value of "tax collection" or "trade regulation."

Within each Employer there is a hierarchy of Employer Sub-Groups. Organizationally, within DHS, those would be the twenty-four organizations reporting to the Secretary. These include components such as Immigration and Customs Enforcement (ICE) and Intelligence & Analysis (I&A) and offices such as Policy and General Counsel. Identifying the Sub-Group narrows the possible attribute values for authorized purpose.

A person may have more than one employer, either because he has more than one job or because he is detailed from one to another. In many jurisdictions it is common for police officers to have security jobs at night or on the weekend; it is possible that either of those activities could result in access to government data. Or, a contractor hired by DHS I&A may get access to intelligence systems that no other person in private industry would get. Or, imagine a US Coast Guard employee detailed to FEMA to provide marine expertise; on any given day, she may need to access systems from both "employers" and will need the ability to deliver either or all of her Employer attributes to an access control evaluator.

b. Employer Type

Some access rules specifically indicate the type of organization which may access information. For example, the Routine Use notice (required under the Privacy Act) for TECS[17] says that information will be routinely shared with state and local government agencies that have the responsibility to investigate violations of criminal law. If an individual has an Employer value of "Department of Public Safety" and an employer type value of "state government" they would meet this access control rule. In a more advanced system, these could be parsed to relevant sub-types for example "Private

[16] Knowing the employer may also mean knowing what sorts of IT security standards the individual's access device has and that also may affect an access decision. This paper, though, is limited to information more tightly linked to the individual.

[17] 50 Federal Register 30048. (Note: the system was named "Treasury Enforcement Communications System" before Customs was transferred to DHS.)

Industry: Contractor: FFRDC" may signal greater authorities than any other type of contractor because employees of Federally Funded Research and Development Corporations may manage government employees while other contractors may not.

c. Employment Type

Possible values for Employment Type include "permanent," "temporary," "detail," "contract," "guest," "volunteer," and "intermittent." This relationship between the employer and the individual is often important for both access and audit purposes. For example, consider the difference between access permitted to a DHS employee and a contractor working for DHS. At the simplest level, if this system were in place, contractors would no longer erroneously receive all of the DHS Human Resources emails (e.g., notices of retirement seminars and changes to HRIT) as they do today.

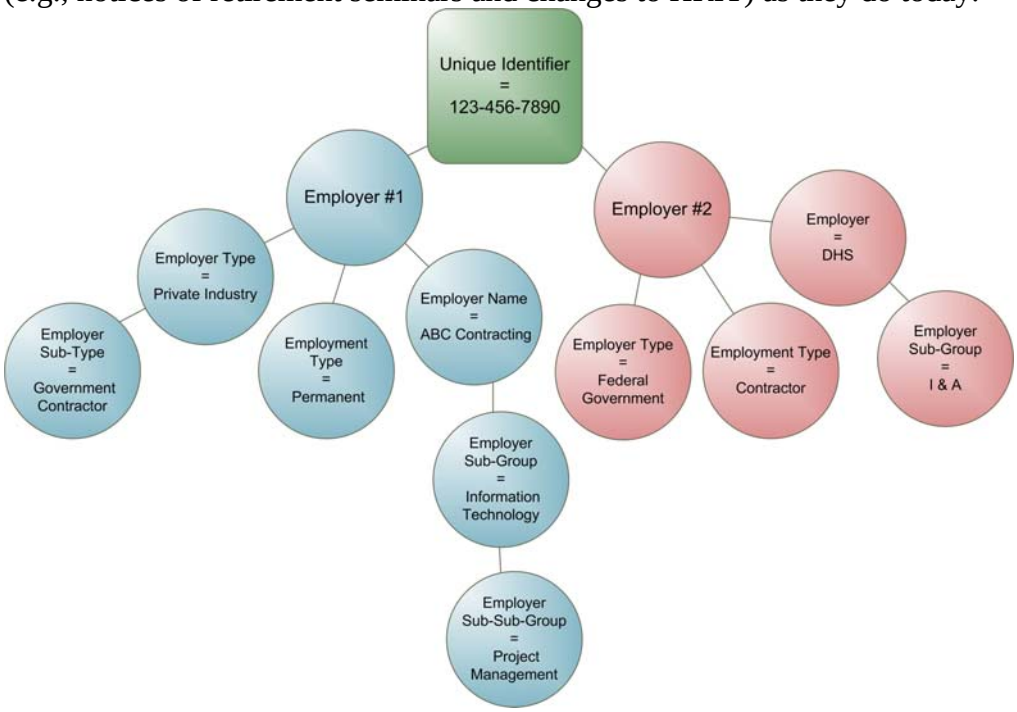


Figure 13 Multiple Entries for Employer

Tracking Employment Type will also address a host of more complex access decisions. With these attributes a system could recognize and handle a wide variety of multi-assigned personnel including: DHS employees who are detailed to other parts of the Department (i.e., a US Coast Guard employee detailed to the Federal Emergency Management Agency to help with marine issues); DHS employees who are detailed to other agencies (i.e., an Immigration and Customs Enforcement agent assigned to an FBI Joint Terrorism Task Force); state or local government employees serving in advisory capacities (i.e., a New York State Police officer serving on the Information Sharing Environment tiger team); or civilians serving in governmental roles (e.g., as active-duty reservists or doctors serving in FEMA's Disaster Medical Assistance Teams).

2. Employment Activities

Table 5 Employment Activities

Attribute	Explanation	Example(s)	Common Source	Maximum # Values / User
Job Designation	designation for a type of work	OPM Occupational Series (1811 = law enforcement), SIC codes	HR system	1
Physical Location	Used for regional access restrictions	Arizona, NY Metro area	HR system, Travel Reimbursements	Multiple
Location Type	Used for regional access restrictions	Permanent, Temporary, Virtual		Multiple

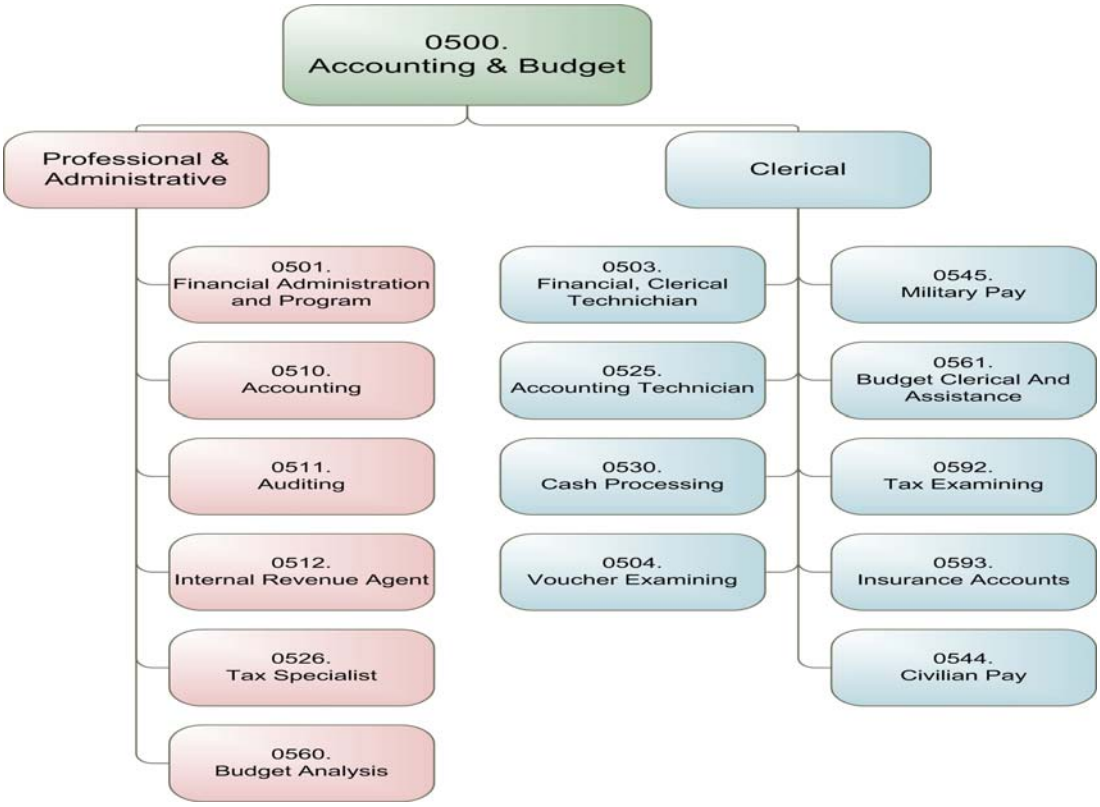
a. Job Designation

More often than not, access to information is controlled in some large measure by an understanding of what work the individual is doing. This is often described as the "mission" of the individual's group. This can be a description as broad as "law enforcement" or as narrow as "granting visa extensions." For the purpose of this project we choose to adopt the Markle Foundation's recommended phrase "authorized purpose" because, in fact, every thing someone in the federal government does is derived from an authority granted by the Constitution. In our system of government, anything not granted by the Constitution (or the Supreme Court's interpretation of the Constitution) is a power that belongs to the states or to the citizenry. Ultimately, every time a federal employee looks at a piece of information and every time the federal government shares a piece of information with anyone else, or intentionally receives a piece of information from anyone else it is because it falls within some Constitutional power.

Unfortunately, we have no recent history of describing government activities in this way. However, there are bits of collected information which serve as proxies. As described in the previous section, knowing the employer and the sub-group within the employer's organization can narrow the choices to one or just a few. Job designations, including job titles and job codes, are others. For example, the Office of Personnel Management divides the work of the federal government into occupational series, job classifications which can provide taxonomies of activity. The 1800 series, for investigators, very explicitly divides them into mission roles (e.g., 1811 = Criminal Investigating; 1815 = Air Safety Investigating; 1816 = Immigration Inspection, and 1822 = Mine Safety & Health).

In addition, the occupational series can correlate directly to access control restrictions. For example, the 0500 series for Accounting and Budget is broken into Professional and Administrative duties. In financial organizations, having tight control over who can

Figure 14 Accounting Occupational Series



access which information and who can alter which information can be the key to reducing fraud and error. With job roles so clearly delineated in this financial series, and the occupational series being included in human resource systems throughout the federal government, it should be quite easy to ensure this sort of access control through user attributes.

There are a number of more detailed pieces of information that would be valuable for granular access control; however related user attributes have been placed in the "second priority" list because there are not consistent digital sources for the information.

b. Physical Location

Access to some information is limited by the geographic region of the employees. For example, the Upstate New York Regional Intelligence Center (UNYRIC) limits access to appropriate state, local, and federal intelligence-related personnel in its region. The FBI's R-Dex (Regional Data Exchange) provides access to federal and local law enforcement personnel in a particular location; the first site was St. Louis. And, the RAINS/Connect and Protect program was limited to Portland, Oregon. DHS' DisasterHelp allows each region to establish its own information sharing group. In federal government systems, the information about a person's physical assigned location is contained in agency personnel systems.

Figure 15 Location Attributes

Location can be defined as a city, a metropolitan area, a state, or a national geographic region. It would be unusual for a system to include all of these different designations. However, the DHS Geospatial Management Office has proposed a project to geo-code all location information in DHS systems. If this activity occurs, any location value could be matched to any location access rule, even if the information was initially incompatible. For example, if the Southwest Border Initiative (SBI) limits access to that region, it would be easy to determine that the geospatial description of Philadelphia is not within the latitude and longitude boundaries of the Southwest.

c. Location type

Most often, an individual's location is the location of the office to which she is permanently assigned. There are times, however, when an individual is detailed to another location or telecommutes to another location. In certain categories of work (i..e., federal emergency response), this is sufficiently common that it should be a primary attribute. For this reason, a Location Type attribute sub-property is also necessary. Unfortunately, many human resources systems do not track temporary travel assignments. However, it may be possible to use travel reimbursement system records as a proxy for Location and Location Type information, particularly if the travel exceeds one month (a typical financial cycle).

3. Employment-related Authority

Table 6Employment-related Activity

Attribute	Explanation	Example(s)	Common Source	Maximum # Values / User
Active Clearances	Access to classified	Secret, Top Secret	Scattered Castles, JPAS,	Multiple

	material, Proxy for trustworthiness		CVS	
Special Authorities/ Special Licenses		Deputized federal officer; Master timekeeper,		
Management Level	Access to policy deliberations;	Supervisor, Program Lead, Senior Executive Team Leader, Military Rank	HR system, OPM job code	1
Direct Reports	In combination with Mgt Level - Authority to validate HR data for others, Authority to override access restriction	By organization code		Multiple
Rating official/ Reviewing official	Persons authorized to validate work assignments, performance appraisals	By organization code	HR system	Multiple

a. Active Clearances

Information which is critical to national security (e.g., foreign counterintelligence, defense, counter-terrorism) is tightly controlled. As described in the "Relationship" section, in order to access such information, one needs to present *bona fides* – both a legitimate business purpose for requesting access and the possession of an appropriate security clearance.

Information about an individual's security clearances can now be readily determined. The clearance attribute values – Secret, Top Secret, etc. – have been long established. But, in the past, agencies often would not give credence to the clearances granted by other agencies and individuals needed separate background investigations, the precursors to grants of clearance, from each agency. Since 9/11, federal policy[18] has shifted to requiring agencies to honor each other's clearances. There are now three authoritative sources for obtaining an individual's clearance information.

Some organizations also use possession of a security clearance as a proxy for trustworthiness. Technically, this is inappropriate because information about possession of a clearance is to be used only in furtherance of national security. However,

[18] See, e.g., Executive Order 13381 (June 27, 2005) (requiring "agency functions relating to determining eligibility for access to classified national security information shall be appropriately uniform, centralized, efficient, effective, timely, and reciprocal").

anecdotally, this informal access rule appears to be used quite often, particularly in person-to-person sharing decisions and in state and local governments.

It bears noting that people sometimes confuse classified information with another set of guarded information. Typically called Sensitive But Unclassified (SBU) or Controlled Unclassified Information (CUI), this category includes information which can be critical to domestic tranquility but which is not related to a foreign threat and, therefore, not able to be classified under the law. Some of the information which can fall into this category is vulnerabilities of nuclear power plants, investigation into public corruption of high level officials, or early stage investigation of highly contagious lethal diseases. Recently, the White House mandated[19] that the Executive Branch establish a consistent set of standards and access controls for such information. This new framework establishes safeguarding levels and dissemination rules. The safeguarding levels are only information about the information and have no corresponding requirement, similar to a clearance, that pertains to the individual. The specified dissemination structure being proposed, is consistent with the concept of attributes and would require the specification of the attributes needed for dissemination.

b. Special Authorities/Special Licenses

In the course of planning and strategy discussions for the Information Sharing Environment, parties often raise a "special" group of individuals of one sort or another, a group which requires different treatment or special access. Often, these individuals have a narrowly granted permission. The single most common example is the reference to "sworn" law enforcement officers; as described in the Proxy section, this is often a reference to their special authority to perform arrests or conduct criminal investigations. In other professions, there are other small groups with special authorities. Such authorities can range from being licensed to prescribe narcotics to being licensed to drive a hazardous materials truck.

At this time, we cannot identify all of the special licenses or authorities which might impact an information access decision somewhere in DHS or elsewhere in the government. To complete such a task may never be possible considering the changing nature of the government and the issues before it.

Initial discussions assumed that each type of special license would need to be represented in a separate attribute property, but it would be more efficient and effective to have a single sub-property which permits a broad range of values. Any value could be included which indicates a special permission granted pursuant to a consistent standard and nomenclature. In structuring a system as is proposed here it does not matter that the values may be disjunctive, entirely unrelated to one another, so long as system access rules define which attribute value is being sought.

[19] Presidential Memorandum for the Heads of Executive Departments and Agencies, Guideline 3 (December 16, 2005)

c. Management

Management roles and relationships are used for a variety of access control decisions. In the employee management arena, depending upon the agency, persons with supervisory authority may access or enter performance appraisal or employee job assignment information as well as approving time records and travel vouchers. In operational environments, supervisory personnel may have special access to approve new projects. Managers of a particular project or subject may have the authority to manually override an automated access denial. And, highest level managers may have exclusive access to systems or files that address policy matters.

Management value attributes are commonly captured in government human resource systems. For example the National Finance Center (NFC) which provides payroll for the federal government offers these values based upon the Civil Service Reform Act:

Table 7 NFC Management values

2	Supervisor OR Manager	Requires exercise of supervisory or managerial responsibilities for application of the General Schedule Supervisory Guide or similar standards of minimum supervisory responsibility specified by position classification standards
4	Supervisor (CSRA)	Position meets the definition of Supervisor in 5 U.S.C. 7103 (a)(10), but does NOT meet the minimum requirements of application of the General Schedule Supervisory Guide.
5	Manage-ment Official (CSRA)	Position meets the definition of Management Official in 5 U.S.C. 7103 (a)(10), but does NOT meet the General Schedule Supervisory Guide definition of Supervisor/Manager or the definition of Supervisor in 5 U.S.C. 7103(a)(10)
6	Leader	Position is titled with the prefix "Lead" and meets the minimum requirements for application of the Work Leader Grade Evaluation Guide or meets similar minimum requirements for leader responsibilities specified by the job standards or other directives of the applicable pay schedule or system. Position is under a Wage System or leads a team performing One-Grade Interval work.
7	Team Leader.	Position is titled with the prefix "Lead" and meets the minimum requirements for application of the General Schedule Team Leader Grade Evaluation Guide; Position leads a team of General Schedule employees performing Twi-Grade Interval work.
8	All Other Positions	Position does NOT meet the above definition of Supervisor or Manager, Supervisor (CSRA), Management Official (CSRA), Leader, or Team Leader

Combining management level attribute values with employer subgroup values, it should be possible to compute all individuals reporting to another individual. For example, hypothetically, if Bob is a 4 (supervisor) of 33614 (subgroup value in employer ABC Agency), then Carol, Ted, and Alice are direct reports if they are 8 (not supervisor or manager) and also are in subgroup 33614. If subgroup taxonomies are well defined, it should also be able to determine indirect reports, people reporting to supervisors who report to other managers.

4. Personal Characteristics

Table 8 Personal Characteristics

Attribute	Explanation	Example(s)	Common Source	Maximum # Values / User
Citizenship	Used for "NOFORN", Access for treaty participants	US, US Legal Permanent Resident, Canada	CIS OPM US Passport Agency	Two?

In many of the government's critical national security and homeland security activities, access to information is limited to US citizens. Most federal employees are US citizens and that information might be confirmable through employing agency or Office of Personnel Management records.

Not all employees of state, local, or private entities are US citizens; pulling individual visa information from DHS/CIS will provide citizenship information for foreign nationals legally working in the United States. One risks, which exists in other methods in place today, is that there is no easy way to identify a foreign national illegally working in the United States if he claims to be a US citizen, since we have no registry of citizens.

In some cases, pursuant to bi-lateral and multi-lateral treaties or agreements, foreign nationals are permitted access to sensitive federal information. There is not a single source of information for verifying foreign citizenship, but for this purpose, data may be available from sources such as Interpol and our own Department of State which credentials foreign diplomats and employees working within the US.

5. Priority Attribute Conclusion

An example of the application of all these priority attributes is shown in the following diagram. As you can see in this example, the DHS-ICE employee is detailed to JTTF at the FBI, which is part of Department of Justice. The two employer attributes have differing employment type attributes, the Department of justice being a detail.

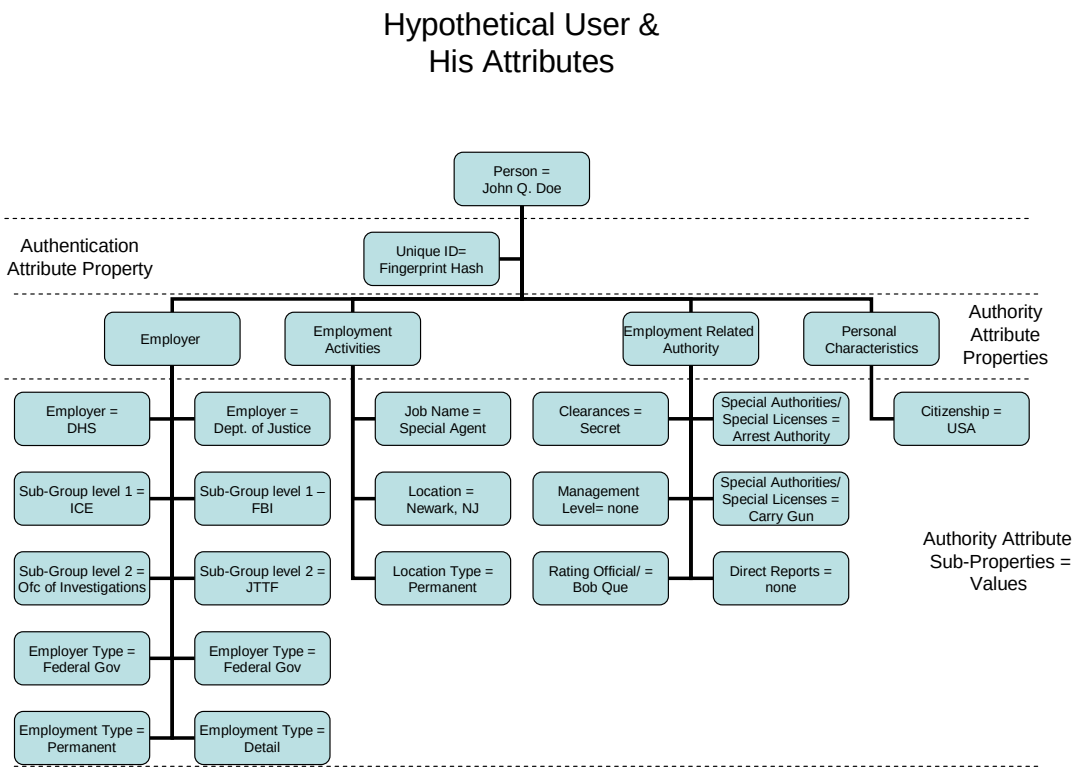


Figure 16 Implementation of Primary User Attributes

iii. Second Priority Attributes

A secondary set of desirable user attributes has been identified. These attributes would permit more flexibility in the access control rules that could be applied. However, these attributes are either ones which only impact a small population (i.e., system administrators rather than system users) or ones which present potentially significant impediments to creating an initial operating capability. The former group would be considered "common core" attributes, while the latter would otherwise be part of the "universal core." Obvious challenges that reduce universal core attributes to secondary priority include attribute values that are not consistently available in current systems. These are values which present challenges so significant that they would likely cause

tremendous delay implementation of IOC.

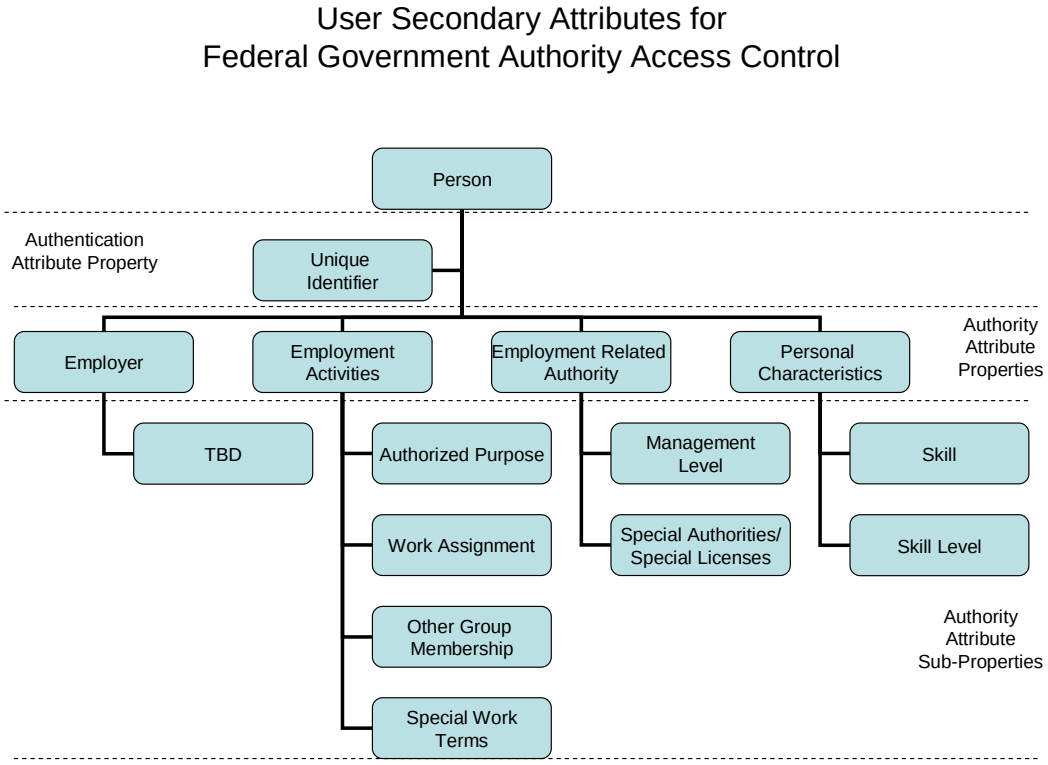


Figure 17 Secondary User Attributes

1. Employer

No additional Employer attributes have been identified. However, because this is likely to occur, this section is left as a placeholder for later discoveries.

2. Employment Activities

Table 9 Employment Activities - Priority 2

Attribute	Explanation	Example(s)	Common Source	Maximum # Values / User
Authorized Purpose	Mission established by law (derived from the Constitution)			Multiple
Work Assignment	Subject/Topic assignments or Individual matter assignments	Al Queda, Mexican border, Enron investigation	Name of work unit; Case or matter files, Program	Multiple

			Management file	
Other Group Membership	May have special access or access limitations	Bargaining unit, Advisory board, Contractor under DD254, Veteran, Background investigated		Multiple
Special Work Terms	Characteristic of employment relationship	Probation, Weekend shift, Disciplined (security violations)	HR system, Time system	Multiple

a. Authorized Purpose

The single most important thing that a holder of information usually wants to know about someone seeking access is what that requestor will do with the information. Generally, this is referred to as the requestor's "mission." As described in the Job Designation subsection, the federal government may only engage in activities which can be derived from an authority granted to the federal government by the Constitution because all other powers are reserved to the States and/or the people.[20]

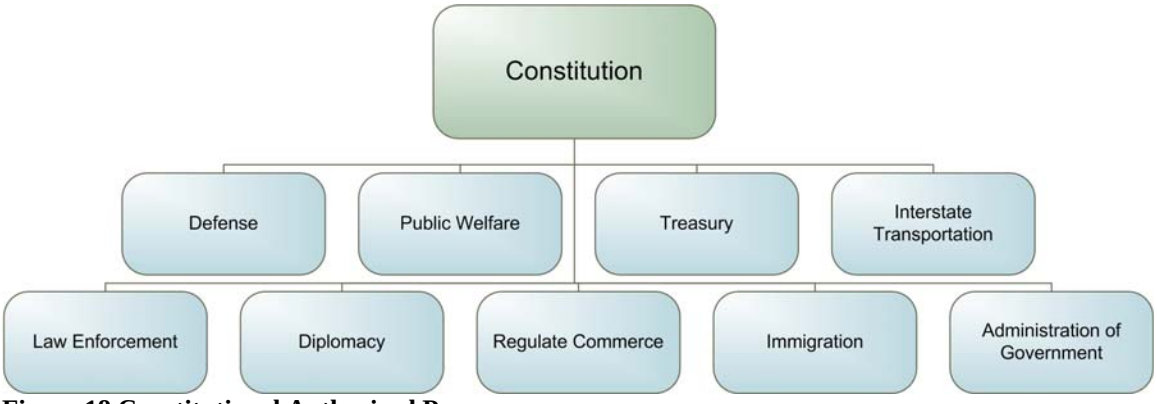


Figure 18 Constitutional Authorized Purposes

Even when deciding whether to share information with a non-federal party, such as a state or private individual, the underlying questions are "Does sharing this information serve an appropriate federal purpose?" or "Is sharing this information within the bounds of the government's authority?" However, for the most part, only a small group of lawyers and policy-makers are consciously aware that this underlies the transaction. On a day-to-day basis most individuals do not think of such things nor do they know the chain of delegations which led to the creation of their current role. The following figure lays out these roles which guide the justifications for the authorized purpose.

[20] Amendment X, U.S. Constitution.

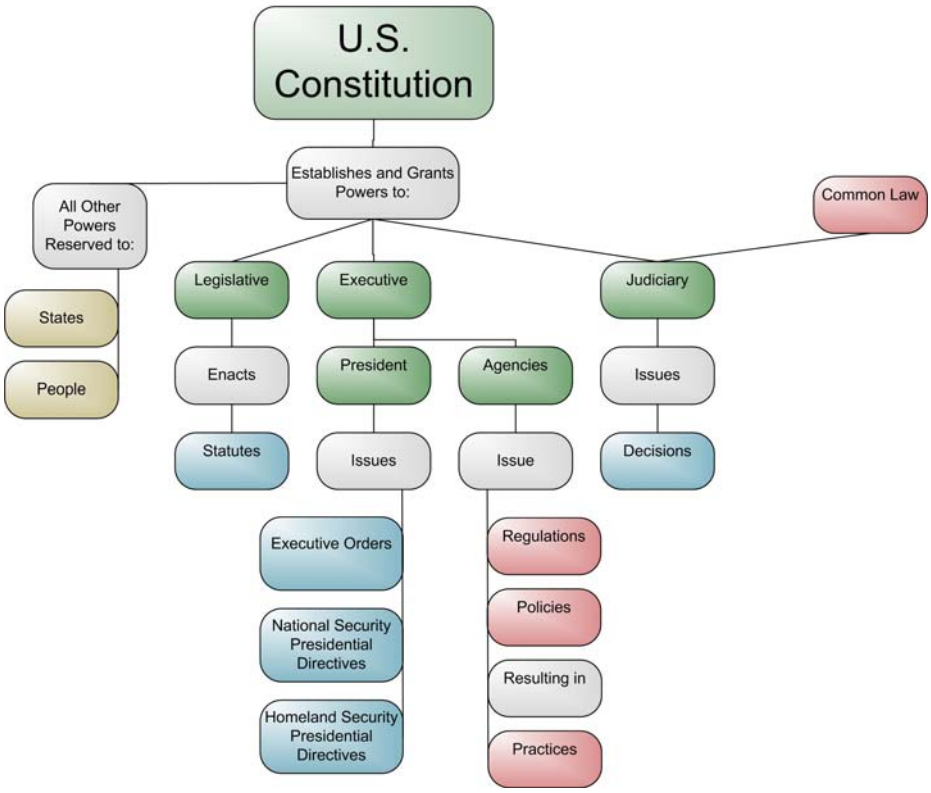


Figure 19 Decomposition Paths of Authorized Purpose

In a perfect information access system, though, this information would be readily available about each individual and the particular work she was doing that caused her to request access. Such information, if given consistent terms would radically improve the level of automation possible, speed of access decisions, granularity of audit, and accountability to the public through generalized transparency.

The Markle Foundation Task Force referred to this critical information sharing indicia as "authorized purpose"[21] and there has been some adoption of the term for the Information Sharing Environment (ISE).[22] Although there are proxies for this information, it is not yet explicitly recorded in any formal construct within the government or its metadata. A detailed taxonomy should be created to describe all of the major Authorized Purpose attribute values and to create a clear structure into which to place the less common ones.

b. Work Assignments

Older "need to know" rules assumed that someone only needed access to information if they were working on the same topic, that only a person working on Al Qaeda needed to

[21] See, e.g., "Increasing the Signal in the Data Noise" subsection of "Creating a Trusted Network for Homeland Security," Markle Foundation Task Force on National Security in the Information Age (Dec. 2, 2003).
[22] See, e.g., "2.3.5 Information Privacy and Civil Liberties Needs," "Information Sharing Environment Implementation Plan," p.22 (November 2006).

see Al Qaeda files. Since 9/11, the view has broadened significantly to recognize that information often has value to seemingly unrelated functions. For example, an ATF agent can only discover a link between a tobacco tax fraud case and a terrorism investigation if there's an opportunity to access the non-ATF case. Nonetheless, there are still matters to which access should be restricted either due to their sensitivity (i.e. Secret Service records of threats on specific individuals) or due to the likelihood of misunderstanding without further explanation (i.e., CIS records on the immigration status of an individual).

c. Other Group Membership

The Other Group Membership sub-property is a catch-all for any other group in which an individual requestor may be a member, where access permissions or restrictions apply to the members of the group. For example, some collective bargaining units in the government have negotiated terms of access. And members of advisory groups, such as the Homeland Security Data Privacy and Integrity Advisory Committee, may have an Employment Type value of Volunteer but have significantly greater access to information than the volunteers who pile sandbags during a flood.

d. Special Work Terms

Another catch-all group, the Special Work Terms sub-property refers to information about the individual's employment that might result in additional access permissions or restrictions. For example, new employees still on probation and employees who have been disciplined might have lesser access than their co-workers. Weekend shift workers might have increased access because they often handle multiple roles in a reduced weekend staff.

3. Employment Authorities

Table 10 Employment Activities - Priority 2

Attribute	Explanation	Example(s)	Common Source	Maximum # Values / User
Management Level	Authority to validate HR data for others, Authority to override access restriction	Matrix management authority, Component Administrator, Programmatic lead		Multiple
Special Authorities/ Special Licenses	Additional values	Master Timekeeper, Systems Administrator, COTR, Training, Licensing Agent		

a. Management Level

There are a number of values for the Management Level attribute sub-property which may be too difficult to capture for IOC. Second priority attribute values include Matrix Manager, Component Administrator, and Programmatic lead. Individuals in these roles, may also have the ability to alter human resources data or to override access restrictions (i.e., give someone by-name access).

b. Special Authorities/Special Licenses

There will be Special Authorities and Special Licenses which individuals possess that affect very few individuals. In order to create highest value functionality first, these attribute values should be deferred to the secondary attribute group. Included are the Master Timekeeper, the Systems Administrator, and purchasing related authorities, such as the Contracting Officer's Technical Representative (COTR). In some cases, having completed special training is required before being permitted to access systems. A value which reflects that completion also could be included in this attribute sub-property.

4. Personal Characteristics

Table 11 Personal Characteristics - Priority 2

Attribute	Explanation	Example(s)	Common Source	Maximum # Values / User
Skills	Skills of the user,	Languages spoken or read other than English, computer languages,		Multiple
Skill level	For each skill a capability score	Fluent (S-4 / R-4), Highly skilled, Qualified	Language Skills Inventory (LSI) used by the Department of State	1 value for each skill

a. Skills

In a variety of work roles, specific skills are needed to be qualified to do certain work. If so, a system would need to deliver two related attribute values for each skill: the name of the skill and the skill level. Although none of the systems reviewed used skills as authority attributes, they were repeatedly mentioned in interviews. Foreign language was the skill most often discussed. The Department of State makes some foreign assignments based upon those skills. And, multiple agencies assign individuals to read and respond to correspondence or questions in other languages; to analyze intelligence information in other languages; etc. As such, it is possible that access to a system or a particular subset or document within a system, may be limited to those with appropriate skills as an added security measure. It is conceivable that a data steward would decide that access to Al-Queda documents in Arabic be limited to individuals who read Arabic in order to

eliminate the risk that a non-Arabic reader is printing the data in order to pass it to an unauthorized user. A similar skill might be proficiency in a programming technique being required to see source code. Other skills have yet to be identified and the authors are unsure of the role that skills truly make in defining access to information. For each skill, a proficiency would need to be established.

b. Disallowed Discriminators

This approach also assists policy personnel to easily review access rules to ensure that no unallowable discriminators are being used. For example, while they may be Authentication Attributes, personal characteristics such as race, gender, and national origin should not be Authority Attributes.

iv. *Implementation Considerations*

In deciding whether to grant access to information, the fundamental questions are always "Which data?" "Which Person?" "Under which circumstances?" As these authority attributes have been defined, they will answer the questions about whom and circumstances. The attribute categories of "Employer" and "Personal Characteristics" describe the person, while "Employment Activities" and "Employment Authorities" described the circumstances.

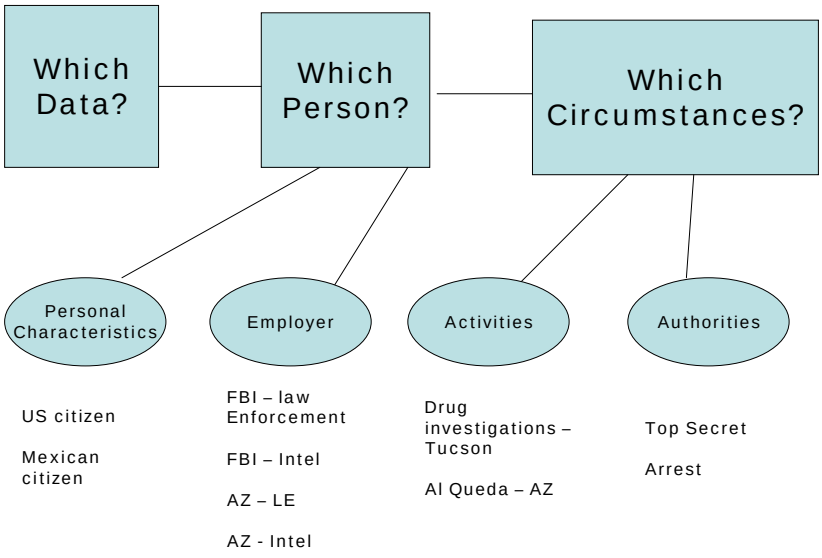


Figure 20 Attribute questions[23]

[23] The above figure also makes clear that this structure could be readily used for interim functionality, while systems are not ready to take so many separate inputs. The attributes, as laid out above, could be translated into concatenated hash codes which would be accessible to more of the currently available technologies.

Additionally, we must reconcile this approach with current ontological approaches to access control. The following graphic shows how primary and secondary attributes track to common and universal core.

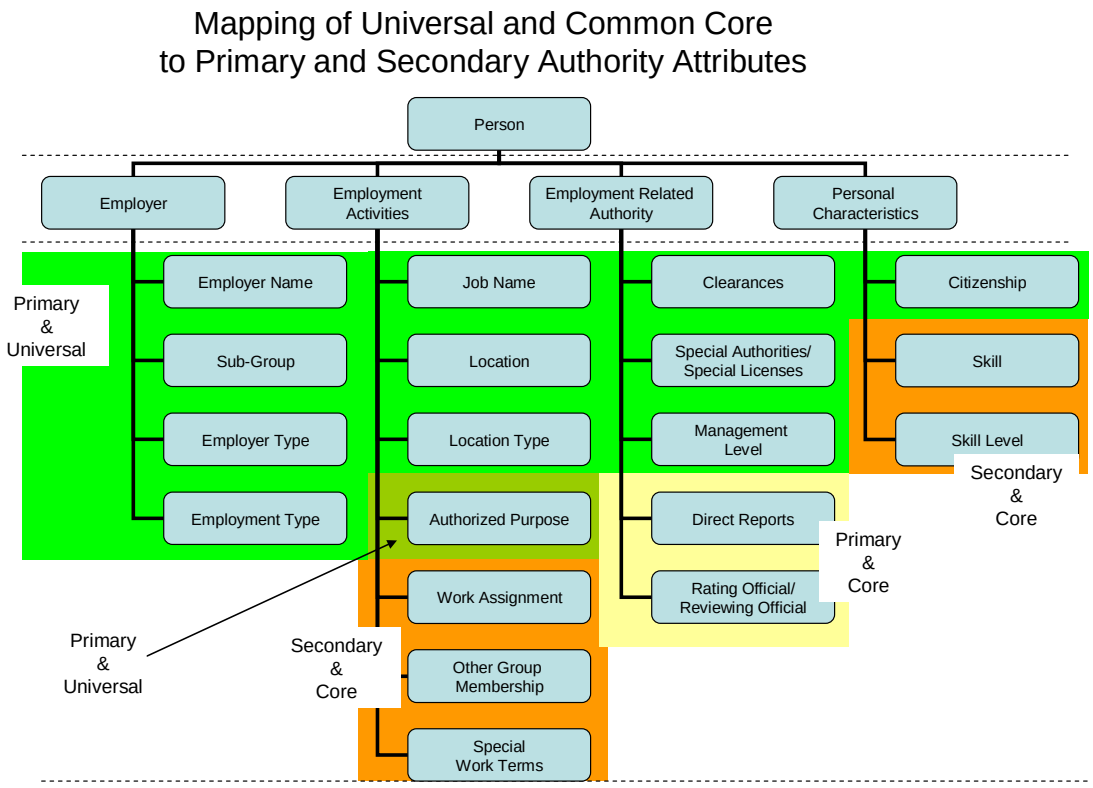


Figure 21 Mapping to Universal and Common Core

5) Authoritative Sources

Each time an access rule needs a user Authority Attribute, the attribute must be delivered from an "Authoritative Source." An Authoritative Source is a digital repository of the relevant information which is collected and regularly updated to meet a business need. For example, a government human resources system is the Authoritative Source for information about whether a person is currently a permanent employee of that agency. But, to determine if a contractor is currently a "contract employee" of the agency, information would have to be drawn from two Authoritative Sources: the company's human resources system would likely be the Authoritative Source for whether the person is a current permanent employee of the company and the agency's financial management system may be the Authoritative Source for whether the consulting company has an active contract. None of these systems is capturing the information for the purpose of determining data access rights; they are collecting the information for the purpose of running the day-to-day business of the organization. These are Authoritative Sources because they are the primary digital source for the information.

i. *Data Quality*

Arguments can be made about why the quality of data in existing Authoritative Sources is insufficient to meet the requirements of an automated access control system. For example, many Authoritative Sources are not maintained in real-time or anything approaching it. Data quality is often not addressed in depth unless the information is already being used to support an automated process for decisions that are deemed important, like payroll. Data that is only considered informational, even in these same databases, tend not to have the same data quality. The need for data quality is apparent when the information is being used for access decisions.

It is important to remember that the standard for judging data quality in the first instance should not be "does the data meet the highest quality standards?" but rather "is the data quality better than what is being used now?" For example, naysayers will point to a human resources system and say that the data quality is not good enough for critical access control decisions because it is only updated bi-weekly, to dovetail with the payroll cycle. Rational thinkers will note that the currently used, static lists are reconfirmed annually if at all. Thus, there will be a vast improvement in data security when a system which may never recognize that the person seeking access to data is a terminated employee is replaced with one that will know of his termination within two weeks. Where Authoritative Sources have been identified in the Attribute Maps, data quality and data update information should be noted in the System Summary when known.

The System Summary also should note whether the data is from a primary or secondary source. A primary source is the system where the information is originally collected and a secondary source is any other system containing the information. Like the children's game of "telephone", the more times the data is passed, the higher the risk that the data quality is reduced. Drawing attributes from a single primary source will be appreciably more effective than the current approach of creating multiple individual sources with data quality issues.

The other point to make concerning data quality is that data quality only improves when the data is used. Unless there is negative consequences of the data being inaccurate it is rarely kept accurate. The current "authoritative sources" may not be as accurate as would be desired for access, as the data is used, if there are consequences of its inaccuracy, the data quality is likely to improve. (Consider graphic showing how this reinforces itself – possible system dynamics graphic)

ii. *Choosing Secondary Sources*

For practical reasons, such as common data structure and related economic efficiency, it may be preferable to accept certain secondary sources in the initial operating capability. For example, the National Finance Center (NFC) is a secondary source but a great wealth

of information. The system is used to generate the federal payroll and is therefore accurate for core pay-related items, such as whether someone is a federal employee, and it is timely to the extent of its biweekly refresh rate. Because of its nearly universal use across the federal government there would be no need for translation tables for data drawn from this system; it could be an acceptable source for any system where the data steward is not currently checking personnel records directly for employment status. Another example is the three aggregating systems for security clearances; while the primary source for clearance information would be each granting authority, these systems are currently used for clearance confirmation.

Conversely, within DHS, there is a Global Address List (GAL), which is a primary source because employees and contractors submit the information about themselves. An instance of the GAL is available to DHS employees and affiliates online. As viewed there, the information is not complete and often inaccurate. In this instance, a secondary source might be preferable.

iii. *New Authoritative Sources*

Over time, new authoritative sources will arise. For example, on August 27, 2004, the President issued Homeland Security Presidential Directive 12, which requires that agencies use consistent standards to authenticate individuals. HSPD-12 addresses credentialing, but the credentialing systems it requires ultimately may be used as authoritative sources. The credentialing systems will retain relevant attribute data. For example, HSPD-12 requires collection of "Organization Affiliation," which is the same as the attribute "Employer." Also, HSPD-12 will collect data which may be used as proxies for various attributes that are collected as part of the standard vetting process of FIPS 201. As an example, there may be a record that the individual has passed some basic screening which may be used as a proxy for a National Agency Check.

6) Mapping Real Systems to the Model

The test of whether the attribute model is sufficient is to break down existing access rules into their component parts and then map each required piece of information to the model. For example, consider the ePerformance system. It needs to know three things about each primary user. Who are you? What kind of user are you – subordinate, supervisor, or manager? Who do you report to/who reports to you? With that information, it can decide which of the following access to provide: which sort of blank performance evaluation form, which evaluation criteria, and whose evaluations you can see.

In order to gain access to the ePerformance system, the first order of information needed is who the person is. We have addressed this only for the primary users. At this point in time we found that system administrators were defined manually by special permission and that at this point in time there are not consistent attributes associated with these positions. Since in these cases, the system administration function was being completed

by a small number of people. The system seeks a user's name and Social Security Number (SSN). These values map directly to the attribute property known as Unique Identifier. Second, the system seeks a variety of information that lets it compute whether the person is, a subordinate, a supervisor, or a manager, the three major user types. That determination is calculated from information such as the individual's occupational series, job title, pay schedule, and grade; these map to the Job Designation Sub-Property of the Employment Activities Property. In the current system, the users type in the information about who reports to whom. However, future systems could perform this information electronically if there was sufficiently detailed information provided in the Employer Subgroup Sub-Property of the Employer Property. That information combined with already available information about whether the individual is a subordinate, supervisor, or manager should make it possible to calculate the relationships.

A spreadsheet, an Attribute Map, was devised that maps each set of rules about a type of user in a separate column. In each box, as much information as is available is provided about how to deliver the relevant values. For example, in the ePerformance system, the information about primary users is often extracted from National Finance Center files; because the NFC performs payroll functions, it has detailed information about individuals. So, a federal government employee's occupational series can be pulled from the PER-HIS file. In circumstances such as this, where the source is known and details are available, the spreadsheet contains that detail: Header/Row Label, Field Name, and Source file. In other circumstances, particularly where access control is currently handled manually, the only known information may be the Value which is sought, such as that the Job Title must be "Attorney" or "Counsel." In those cases, an effort will be made to identify an Authoritative Source and obtain a data dictionary so that the additional details can be provided.

In order to make clear what is being mapped, a four-color code has been established. Text in black represents mandatory minimum data needed to make an access decision that is already being collected digitally. Text in blue is secondary ("nice to have") data needed to make an access decision that is already being collected digitally. Text in grey is data that is being digitally collected for access control, but which our team has determined may not be required, identified in this manner to reach the optimal number of properties. Text in orange is recommendations for digital collection that does not yet occur.

7) Benefits

Multiple benefits will be derived from building an access control system that knows which user attributes are needed to fire which access rules and that can dynamically reach to authoritative sources to obtain best available user attribute information. Throughout this paper, we have talked about the enhancements to security – right information to the right people – and the increase in speed – at the right time – that would be achieved by such a system.

a. Optimal Access Community

The information gathered through this process can contribute to a performance baseline for information sharing of the particular data. When all the needed user attributes are known for a set of data, the universe of possible users can be defined. For example, a given system might support access, depending upon circumstance, for persons with user attribute values of federal, state, and local government; law enforcement; organizational records management personnel; congressional staffers; and the media. If all the relevant user authority attribute properties become known for a system or set of data, it will be possible to quantify the maximum allowable distribution.

The maximum allowable user community is defined as the user pool that complies with all of the authority access rules. In order to define the maximum allowable user community, the following is needed for each system:

- All authority attributes used by the data steward's access rules
- Semantic standardization of the form in which the attributes are evaluated and collected
- An authoritative source from which the attribute information can be assessed with
    - Approval to access the attribute information
    - Acceptable data quality and refresh rates for all attributes within the authoritative source

For each system we studied, the current user community is smaller than the maximum allowable user community.

As the primary and secondary attribute sets imply, it is unlikely that a 100% solution will be implemented at one time. The primary authority attributes identified in Section 4 were chosen based on the frequency of their use and their availability. As is obvious from earlier discussions, not all of the users are likely to be equally frequent or have equally broad access. Those distinctions are likely to be determinable based upon the context portion of the access rule (e.g., the very frequently used and more readily calculable "in pursuit of a criminal investigation" as opposed to the infrequently used and difficult to determine "when a determination is made that release to the public will advance a criminal investigation"). Thus, the "optimal user community" is not the maximum allowable user community.

The determination of an optimal user community should not be based solely on the numbers of people in a community. For example, if a system has access rules that would permit access to the 600,000+ state and local law enforcement officers around the country and the 12,000 Special Agents of the FBI, it should not be assumed that the state and local community is the higher value community to be engaged first. The information must be placed in context. What if the system is an FBI work-a-day system and the state and locals only have access permission when they are working on a related case? What if al the attributes for the 12000 special Agents of the FBI can be obtained from one authoritative source, and the attributes for the 600,000+ state and local law enforcement officers around the country would require outreach to 5000 jurisdictional databases for authoritative sources. The raw numbers of maximum communities must be put in the

context of such factors as most frequent likely use, highest value of the related work, and ease of implementation. Because it is anticipated that dynamic availability of attribute values will grow incrementally, it is expected that optimal user communities will be recalculated as new attributes are made available.

It should be noted that once optimal user communities are defined, target marketing can occur and performance metrics can be tracked. Statistics can be generated to determine the maximal size of those groups and comparisons can be made between that maximum and the current active user set. For example, if the optimal user community for a system is all disaster workers in the United States, it is possible to research how many people work in each of the component role groups (e.g., firemen, EMTs, FEMA operations, etc.). Because people are presented by unique identifiers, it is possible to determine how many different individuals are accessing a system, and what percentage of the optimal community they represent. And, where the optimal community contains multiple role groups it is possible to break-out the statistics and determine which groups are most under-represented and to establish targeted marketing strategies. In the prior example if firemen were under-represented, perhaps the data steward would attempt to have an article or notice placed in the regular publications of the states' fireman associations. And where there is single sign-on or federated query capability, the fastest marketing may simply be to include the system on the list of options for access.

b. **Mission Value**

As with any project, it is important to understand its value to the organization. The anticipated value of converting system access from current methods to the attribute method must define the metrics with which to measure information sharing: We believe that success will be measured by the increase in the ability to:

- Access[24]: Optimal Access Community- Current Access Community
- Analyze: Mission role of (Optimal Access Community- Current Access Community)
- Act: Improvement to mission based on increased communications

i. ***Increased Access***

The first step in information sharing is increasing the ability to access the information. As is seen in the preceding discussion, the ability to fine-tune access control increases the access community (the population who can access the information). This fine-tuning makes it possible to give the information to all of the people who need it while ensuring that it remains possible to control the information as required. And, specific metrics of optimal community and actual community can be tracked.

[24] This three step process was developed by the DHS, Information Sharing and Collaboration Office as the value chain for Information Sharing.

ii. *Better Informed Analysis*

After access to information is addressed, the information must be put into context to give decision makers the fullest picture available to them when making decisions. If information is appropriately set in context this will increases the quality of decision making. In the end, the benefit will be judged by the ability to take action on the information. Our ability to appropriately Analyze and Act are constrained by whether mission components obtain access to the information they need.

iii. *Better Informed Actions*

Implementing attribute-based authorization will not make ineffective systems more effective but it can systematically increase the effectiveness of existing systems by ensuring that they can be used by those who would benefit and have authority to use the system and allow all users to use the largest set of relevant data in all decisions.

iv. Other Benefits

Implementation of the recommendations in this report should lead to additional specific benefits. It would remove the need for each system to develop an individualized set of access criteria and collect and maintain the user data associated with these criteria. Based on the current list of FISMA systems, which are defined to be the mission critical systems this would consolidate hundreds of system access systems, and significantly reduce the associated management costs.

Over time, it would create semantic standards that are scalable and would allow increases and diversity in the user base with the identification of authoritative sources for their attributes. And, translation costs, currently a significant expense, would be reduced as semantic harmonization grows among the attribute sets. The availability of the data in standard forms would increase the ability to analyze the user data across systems.

It would improve security by memorializing the access rights for individuals in data while providing the ability for updating to address other valid operational needs. Safeguarding is critical because release of information can jeopardize operational activity.

The availability of the data attributes could be used to tailor work flow, presentation, and other system capabilities currently not attempted.

v. Federated use of Authority-based Access

Although the promise within an agency is quite extensive, the biggest opportunities are those in Federated Identity Management. The challenge is one of scale in proposed architectures, such as the Information Sharing Environment that will make it possible to

appropriately and securely share terrorism, law enforcement, and homeland security information both across the agencies of the federal government and more broadly with state, local, tribal, foreign, and private partners. Parallel efforts such as the National Health Information Network, and other Academia and Private Industry enterprises, face the same issues of trust. Authority based attributed make the access rules transparent and allow unrelated systems to communicate accurately the authorities of their users.

8) **Recommendations for Future Work**

Our work appears to provide support for a breakthrough for access control in the government's highly distributed environment. We believe that we have shown that the ability to dynamically call a very few attributes – there are only 13 "primary" attributes in our model – will fulfill the underlying needs of most access control rules within the federal government and between the federal government and its partners. These attributes are tractable and reusable. They are sufficiently basic that they are likely to be available even in very small partner organizations. And, most are clustered in a small number of authoritative sources, reducing the cost and increasing the practicality of building dynamic call functions. Beyond that, we have identified six additional attributes which would further enhance the granularity of access grants or extend the availability of dynamic access control to systems with more unique requirements. We strongly recommend continued work, gathering additional access rules and mapping additional systems, to refine the attribute list and to begin proof of concept access control systems.

This project should be viewed as a first step towards identifying attributes needed to evaluate the practicality and economic viability of providing dynamic calls for user attributes in access control systems. The small number of tractable, highly reusable attributes that provide the needed information to most authority-based access control systems in this review is promising. Although we analyze 4 systems in the appendices, throughout this project we have spoken to many system owners to attempt to identify attributes outside of the less than twenty we have identified and have been struck with the similarities in the authority attributes across systems. The diversity of the systems reviewed in detail give us a degree of confidence in the ability to track each rule/role/access decision back to the authority attributes.

There is still much to be done in implementing an approach of this magnitude. The following, many of which have been defined earlier in this document, is a set of projects that would advance the theories presented and move towards an implementable solution:

- Semantic standardization of access attributes (a significant step in this direction is being accomplished by the Global Federated Identity Management Program)
- Key communities, such as DOJ and DHS, should develop harmonization or equivalency tables across these a barriers
- Evaluation of additional systems to test the current primary and secondary attributes
- Additional collection focused on refining the ontologies and building the taxonomies.

- Find/build sources for second priority attributes
- A separate project to build a federal mission/authorized purpose taxonomy
- A specific project to determine the attribute components of “sworn law enforcement”
- Pilot testing the authority based access approach in a set of systems within a large organization and in a federated environment.
- Conducting a more thorough analysis of the benefits of this approach and the economic drivers of federated access control on a grand scale.

We encourage others to support efforts in this vein and are encouraged by the current efforts in the community in this area.

Appendices

a. Appendix A – Data Collection Worksheets Packet

Attribute Identification Project
System Overview Worksheet

		Source of Info
System Name		
Brief System Description		
Component System Owner		
POC		
POC email		
POC telephone		
Data Dictionary	Requested on _____; Requested from _____; Received on _____	

Attribute Identification Project
System Administrator Worksheet – p. 1

		Source of Info
Sys Admins	Number_____; Are all Sys Admins DHS Employees?: ___; If no, employees of where?: _____; If yes, employees of which components/subcomponents? _____	
Current Users	Number_____; Are all users DHS Employees?: ___; If no, employees of where?: _____; If yes, employees of which components/subcomponents? _____;	
User Authorization	Does Sys Admin decide whether requestor is entitled to user account? _____ If no, who decides? _____	

Attribute Identification Project
System Administrator Worksheet – p. 2

Current Access Rules / User	List Access Rules currently used to decide whether to grant a regular user account:	
Current Access Rules / Sys Admin	List Access Rules currently used to decide whether to grant a system administrator account:	
Current Access Rules / Temp	If there is a temporary or guest account, list Access Rules currently used to decide whether to grant such access:	

Attribute Identification Project
Legal Worksheet – p. 1

		Source of Info
Lawyer for the System Owner		
Access Rules in law		
Privacy Act Access Rules (& citations)		
FISMA requirements (& citations)		
E-authentica-tion requirements (& citation)		

Attribute Identification Project
Legal Worksheet – p. 2

Information Sharing Access Agreement requirements (& citations)		
Federal regulation requirements (& citations)		
Departmental policy requirements (& citations)		
Component policy requirements (& citations)		

Attribute Identification Project
User Worksheet

		Source of Info
Individual User Rules	To whom do you (would you) provide information from the system? _____ Why? _____ (If not otherwise provided, attempt to establish whether there is something about the role of the person which drives the deicision.)	
Individual User Rules	To whom do you (would you) provide information from the system? _____ Why? _____ **(Repeat until user has no more examples)**	
Individual User Rules	To who have (would you) deny information from the system? _____ Why? _____	

Instructions for User Access Rules Interview

When you meet a user, remember that he or she has not been thinking about this project and may not be generally familiar with system development philosophies or law. Your goal is to draw information from the user that he or she may never have thought about.

Treat the meeting as a conversation; be relaxed and explain what you're asking and why.

Keep one eye on the time. Make an effort to be responsive but brief, leaving most of the time for the user to speak. In most cases, you'll want the interview to take no more than one hour.

- Begin with a two or three sentence introduction of yourself and your background.
- Briefly explain the project. Remember to describe it in terms that are meaningful to the user. You don't need to use this language, and we'd suggest you use something in your own words, but there an example is on the next page.
- Ask what the individual does in his/her job
- Ask when they use the system
- Ask whether they provide information or get information or both
- If they get information, what sorts of ways do they usually share it
    - Include it in a written report?
    - Tell co-workers?
    - Use it in a meeting presentation?
- Have they ever gotten information from the system for a co-worker or boss
    - Who was out of the office and couldn't log on?
    - Whose password had expired and needed tech support reset?
    - Who was detailed to the office (not permanently assigned)
- Have they ever been asked for information from the system that they would have shared but didn't know or couldn't access?
- Have they ever had someone ask for information from the system that they thought they shouldn't share?

Sample Project Explanation for User Interview:

"We are working on a project that's one piece of the technology that will let you log on one time, enter one password, and get to every system you need to reach. Then, you won't have to remember lots of ids and passwords, won't have to use multiple computers. Our project is to try to understand all the different ways that a decision is made to give someone information and see if we can account for all of them.

Imagine that this building was like a secure facility you see in the movies and that everything was locked separately. Imagine that we wanted to make a smart card that had enough information to know every corridor, room, person and file you would need to access to do your job. Who would tell us what all those things are? We know we could ask your boss. But, we also know that even the best informed manager in the world doesn't know every way that an employee gets the job done.

In our project, we're not looking at a building; we're looking at information. We know we can ask system designers and lawyers who has or should have access to the information, but we also know that their answers may not be complete. They may not be aware of all the ways information gets used. So, today, we want to ask you about using [name of system]. We want to understand what sorts of tasks you do with the system; what kind of information you get; who you tell that information to (whether in a one-to-one conversation, in meetings, by phone, in emails, or even formal reports). We want to know if people ask you to get information for them (could be your boss, your co-workers, or someone from another group) and how you decide whether or not to do it. We're not asking for the information itself, just to learn about how it moves around.

We're trying to understand what rules get applied, not necessarily written rules, but the ones in your head: 'I would never do this' or 'I always do that' sort of thing. That's just the beginning for us. Once we have a rule, we try to identify the specific thing or things we would need to know about a person in order to decide whether they should get the information. If we had to fill in for you, what would we need to know to make the right decision? We call those "attributes." And, once we know what sort of attributes we're looking for, we will try to figure out if there's another computer system that has the information. For example, if you only give information to people who work for DHS, the "attribute" is "employer." If you only give information to people who work on law enforcement or human resources, then the attribute is "job role."

b. Appendix B – System Maps & Summary Sheets

Appendix B-**1**

Summary – ePerformance

System - The ePerformance system provides a mechanism for employees to receive their performance standards, goals, and evaluations online.

Primary User Roles: The system recognizes three types of users: subordinate employees, supervisors, and managers. Employees can see the evaluation information, while supervisors and managers can enter evaluations and set incremental goals.

Current Access Control Rules: This system determines which user role is appropriate for a person based upon a variety of information. Studying the structure and handling of the inbound data, some access rules can be extrapolated:

- Primary usage is restricted to DHS employees. (Data is extracted about users from the National Finance Center's Personal History file.)
- Union employees are excluded (Subordinates are defined as non-bargaining unit employees.)
- Senior executives do not receive a plan through this system. (Pay plans EX, SL, ES are identified as NO-PLAN.)
- All other employees are identified as an employee, supervisor, or manager. (This determination is generated from an individual's Occupational Series, Grade, Pay Plan, and Supervisor Code).
- Access to any particular individual's performance data is generally limited to that individual and his management.

Attribute Information: ePerformance has already identified the National Finance Center, the organization that creates federal payroll, as the authoritative source for the data it needs. ePerformance extracts data from an NFC personal history file and has identified the data fields it needs for most of the access determinations for its primary user group. Those data fields have been mapped to the User Attribute Properties and Sub-Properties in the following User Attribute Map. In most cases, the system will accept any Value in a selected field. For example, there is no GS grade which is forbidden access, so it will accept any value for the User Authority Attribute. The individual fields that can be extracted from NFC provide clues to a person's managerial status, but no single field provides conclusive information; ePerformance uses these extracts as partial proxies and then performs multiple calculations to reach its determination.

Recommendation :

1. The system does not automatically determine reporting relationships, which person reports to which person. This may be possible to do if individuals' organization codes (identifying sub-groups within the organization) are kept current through as many of the eight available hierarchical levels as are needed.

2. Some of the fields collected may not be needed to determine access. For example, with a unique identifier as strong as a Social Security Number, there should not be a need to capture a person's gender and race as part of the user access information.

Other Data Access: In the System of Records Notice (SORN) required by the Privacy Act, ten other circumstances are identified in which data from the ePerformance system will be given to one or more people.

Current Access Control Rules: These "routine uses" include situations such as giving information to law enforcement officials in pursuit of a criminal investigation or to a congressional office making the request for a constituent's data on behalf of that constituent. The list appears on a separate attached page.

Attribute Information: At present, these types of access are addressed manually. This project attempted to break down each rule into the components needed and has mapped the values sought into the following User Attribute Map.

Recommendation :

1. Because much of the needed user attribute data is about people other than federal employees, more work is needed to identify the types of authoritative sources that exist and common data field names.

Routine Uses permitted for ePerformance Data[25]

A. To the National Finance Center, United States Department of Agriculture, to update employee personnel records and meet government record keeping and reporting requirements.

B. When a record, either on its face on in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil or administrative, the relevant records may be referred to an appropriate Federal, State, territorial, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting such a violation or
enforcing or implementing such law.

C. To a Federal, state, tribal, local or foreign government agency or professional licensing authority in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance or status of a license, grant, or other benefit by the requesting entity, to the extent that the information is relevant and necessary to the requesting entity's decision on the matter.

D. To the news media and the public where there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of the Department or is necessary to demonstrate the accountability of the Department's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in
the context of a particular case would constitute an unwarranted invasion of personal privacy.

E. To the National Archives and Records Administration or other federal government agencies in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

F. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

G. To the Department of Justice (DOJ) or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (a) DHS, or (b) any employee of DHS in his/her official capacity, or (c) any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the
employee, or (d) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that disclosure is relevant and necessary to the litigation.

H. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

I. To an agency, organization, or individual for the purposes of performing audit or oversight operations as authorized by law.

J. To the Equal Employment Opportunity Commission, Merit Systems
Protection Board, Office of the Special Counsel, Federal Labor Relations Authority, or Office of Personnel Management or to arbitrators and other parties responsible for processing any personnel actions or conducting administrative hearings or appeals, or if needed in the performance of authorized duties. Policies and Practices for Storing, Retrieving,

[25] Extracted from System of Records Notice, 71 FR 63329.

Appendix B-2

Summary – DHelp

System - The DisasterHelp (DHelp) system is a portal which allows persons responsible for disaster management to share information within their professional communities and to the public.

Primary User Roles: The system primarily recognizes three types of users: members of the public; registered users; and validated registered users. Registered users can personalize their content. Validated registered users can join specialized communities of interest; can participate in collaboration areas; and can access a White Pages of other validated users.

Current Access Control Rules: This system has a limited number of universal access control rules.

- Public: Members of the public can access general information without providing any unique identifier information.
- Registered: Members of the public and the disaster management community can customize the information they view if they provide basic identifying information (name, email, and zip code).
- Validated Registered: Members of the disaster management community can access one or more Collaborative Operating Groups (COGs), which provide limited distribution information, by providing information that validates their relationship to that category of information (name, email, address, phone, organization, type of organization, role).

In addition, each COG can establish access control rules:

- Generally, these rules define the specific sector of the disaster management community which may access the particular COG.

Attribute Information: In order to be an easily managed, easily accessed system, a very limited set of attributes is sought:

- Public: There is no access control for public access.
- Registered: Registered users must provide their name, email, and zip code.
- Validated Registered: Validated registered users must provide their name, full address, phone number, email, organization, organization type, and role.

Additional information may be gathered (e.g., domain id, IP address), but this is not necessary to access. It may be used for audit or other security purposes.

Recommendation:

1. Because name information tends to be a weak unique identifier, it is recommended that a more robust identifier be collected.
2. Information about address and telephone are not likely to be relevant to access decisions, except to the extent that they provide a proxy for location geo-coding.

Authoritative Source: At present, all information is collected manually.

Recommendation :

1. Because much of the needed user attribute data is about people other than federal employees, more work is needed to identify the types of authoritative sources that exist and common data field names

Appendix B-3

Summary – WebTA

System - The WebTA system provides a mechanism for timekeepers to input and supervisors to approve employees work time and leave online.

Primary User Roles: The system recognizes eleven types of users: employee (not always allowed), timekeeper, master timekeeper, master timekeeper –restricted, master timekeeper – read only, HR administrator, administrator, supervisor, master supervisor restricted, master supervisor global and program managers. Employee is not always allowed as a user type, in some instances employee is simply data and the lowest level user is timekeeper. Timekeepers track time and attendance, supervisors certify the time and attendance record. Administrators address system configuration, build management and managing employees roles and role assignment on a global level. Project Managers address accounting codes and hierarchy. The HR Administrator manages the leave transfer program, manage role assignments, edit and add organizations to the org tree edit and add accounting data and manage employees within their agency. Master level users with read only or restricted access are only at the agency level, not lower organizations.

Current Access Control Rules: This system determines which user role is appropriate for a person based upon a variety of information. Studying the structure and handling of the inbound data, some access rules can be extrapolated:

- Primary usage is restricted to DHS employees.
- Supervisors are defined manually (SUP_ID associated with EMP_ID in TA_USER).
- Timekeepers are defined manually (TKP_ID associated with EMP_ID in TA_USER).
- Delegates are defined manually (DELEGATE_FOR links to EMP_ID)
- Access to any particular individual's time and attendance data is generally limited to that individual, their timekeeper, their supervisor and the HR administrators.

Attribute Information: WebTA is manually updated. The volume of account changes is considered small. The system sends information to the National Finance Center, the organization that creates federal payroll.

WebTA is an original source for much of this data. The core data is employee ID which links to social security, timekeeper ID and supervisor ID. The other fields are often not addressed except to show a change within a pay period. The data fields have been mapped to the User Attribute Classes and Properties in the following User Attribute Map. In most cases, the system will accept any Value in a selected field. There is no known relationship between an individual and their timekeeper that could be identified other than manually. At this point in time the role of the timekeeper is not consistent. If their was a consistent assignment of this task, such as to the supervisors' senior administrative person, this role may be able to be defined externally or used to define attributes

Recommendation :

1. Web TA is a primary system completed as part of an individual's check-in to DHS. It feeds information to NFC for payroll and should be considered for an authoritative source. The system has many characteristics of a quality authoritative source, since it is needed for an important task (payroll) and in most cases entered by someone that is personally aware of the individual.
2. The related supervisor ID with an employee ID could establish a managerial hierarchy that could serve as an authoritative source.
3. The project manager role and accounting codes may be used to establish project leads.

Other Data Access: The System of Records Notice (SORN) required by the Privacy Act is not yet finalized.

Appendix B-4

Summary – HSIN (COIs)

System - The HSIN Community of Interests are self governed access bodies. Each community is established by the users and the rules of the group are self defined. There are currently close to 500 communities of interest in the HSIN system. We looked at four communities of interest (Law Enforcement, State and local Intelligence, Pandemic Influenza and Coast Guard) but learned about additional COIs that are managed by the same COI leads. Information was gathered on the following COIs:

- State and Local Intelligence
- Law Enforcement
- Pandemic Influenza
- Coast Guard Command Center
- National Operations Center (NOC)
- Emergency Management
- Federal Operations
- National Capital Region
- Joint Federal Operations
- Prima Federal Official
- Intelligence Coordination Center
- National Response Center
- Homeland Security Task Force – South East

Primary User Roles: All users within a COI have access to all of the information within the COI.

Current Access Control Rules: This system does most user access manually through policy determinations outside the system. Many COIs have eligibility requirements. In general, the HSIN eligibility for a given COI is that the user is a member of a given community and is actively engaged in the core activity of the COI. In many cases this is based on organizational affiliation.

Some COIs have rules on physically checking the identity and/or credentials of an applicant before giving access to the system.

- Primary usage is restricted by each COI and is collected, reviewed and vetted independently.
- There is open access to information within a COI when given access.
- Many users have access to multiple HSIN communities of interest. If a user has access to multiple COIs, the information, vetting procedures and access for each COI is separate.

Attribute Information: Each COI has a vetting group or official that obtains attribute information for the COI. The current attributes have been mapped to the User Attribute Classes and Properties in the following User Attribute Map. In many cases, the COIs require the same attributes, they simply want different values for these attributes.

Recommendation :

4. The vetting rules are often not well defined and would benefit from understanding the underlying attributes to gain access.
5. Some access rules are based on membership in existing working groups. In general, the attributes of those in the working group are not well defined.
6. In some ways the COIs establish close to 500 roles for data access. The COIs repeat data storage and do not efficiently ensure data availability to those who may access the data.

Other Data Access: In the System of Records Notice (SORN) required by the Privacy Act, claimed exemptions to Privacy Act rules based on law enforcement and intelligence rules.

						ePerformance - Attribute Properties					
						Primary	Secondary				
						System Users	Routine Use Recip				
Attribute Relationship	**Attribute Class**	**Explanation**	**Sample Values**	**Common Source**	**Maximum #**	**Roles: Employees (non-bargaining unit), Supervisor, Manager**	**National Finance Center**	**Law Enforcement**	**Human Resources**	**Media / Public**	**NARA**
Primary											
Unique Identifier	Unique identifier	Linking mechanism to attributes	Name, Fingerprint, Hash code, SSN, Employee ID #, RSA Token	HR system,E-Authentication	Multiple	Header Row Label = LstNm, Field = NAME-EMPLOYEE-LAST, Source = NFC-PERHIS; Header Row Label = MdNm, Field = NAME-EMPLOYEE-MIDDLE, Source = NFC-PERHIS; Header Row Label = FstNm, Field = NAME-EMPLOYEE-FIRST Source = NFC-PERHIS; Header Row Label = SSN, Field = SSNO, Source = NFC-PERHIS	Value = [any]	Value = [any]	Value = [any]	(not needed for public)	Value = [any]
Employer	Employer	Proxy for list of possible authorized purposes.	DHS employee = "immigration administration" or "law enforcement" but not "tax collection"	HR system, Agency finance system (for contractors)	Multiple –	File Name = DHS_PP##_YYYY.csv, Source = NFC-PERHIS, (PROXY FOR "Value = DHS");	value = Department of Agriculture				Value = "NARA" or if authorized purpose value is correct
Employer	Employer Subgroup	Narrows proxy list of possible authorized purposes	I&A = intelligence, ICE/Gangs = "law enforcement" sub-purpose = violent crime"; "drugs"; "organized crime"	HR system	Multiple	Header Row Label = DeptNum, Field = ORG-STRUCTURE-CODE; Source = NFC-PERHIS; Header Row Label = OrgLevel1, Field = ORG-STRUCTURE-CODE-AGCY, Source = NFC-PERHIS; Header Row Label = OrgLevel2, Field = ORG-STRUCTURE-CODE-2ND-LEV, Source = NFC-PERHIS; (REPEAT including OrgLevel3 through OrgLevel8)	Value = National Finance Center **and** value= group that updates personnel records or group that does records management or group that does records management reporting				

Employer	Employer Type	Establishes relationship of organization to the federal government	State government, local government, Private industry, Foreign government		1			Value = "federal government," "state government," "territorial government," "tribal government," "local government," "foreign government," or "international organization"	Value = "federal government," "state government," "territorial government," "tribal government," "local government," "foreign government," or "professional licensing authority"		Value = "federal government"
Employer	Employment Type	Establishes relationship of individual to the federal government	Permanent, Temporary, Detail, Contract	HR system, Agency finance system (for contractors)	Multiple	Header Row Label = EmplStatus, Field = CURRENT-EMPLOYEE-STATUS, Source = NFC-PERHIS					
Employment Activities	Job Designation	Formal nomenclature describing the individual's job; may be proxies for authorized purpose	Occupational Series = 1811 = law enforcement, Attorney, Special Agent	HR system	Multiple	Header Row Label = OccSeries, Field = OCCUPATIONAL-SERIES-CODE Source = NFC-PERHIS (USED TO CALCULATE "Calculated Cluster" which is USED TO CALCULATE "Supervisor Code"), Header Row Label = Jobcode, Field = MASTER-RECORD-NUMBER, Source = NFC-PERHIS: Header Row Label = Work_TTL_Cd, Field = WORKING-TITLE-CODE Source = NFC-PERHIS (USED TO CALCULATE "Supervisor Code"); Header Row Label = PayTable, Field = PAY-TABLE-CODE, Source = NFC-PERHIS		value = 1800 (if "federal government")			
Employment Activities	Physical Location	Used for regional access restrictions	Arizona, NY Metro area, Southwest	HR system,	Multiple	Header Row Label = DutyLoc, Field = DUTY-STATION-LOC-CODES, Source = NFC-PERHIS					

Employment Activities	Location Type	Used for regional access restrictions	Permanent, Temporary, Virtual	Travel Reimbursements	Multiple						
Employment Authorities	Active Clearances	Access to classified material, Proxy for trustworthiness	Secret, Top Secret	Scattered Castles, JPAS, CVS	Multiple						
Employment Authorities	Special Authorities, Special Licenses		Deputized federal officer; Master timekeeper								

Employment Authorities	Management Level	Access to policy deliberations;	Supervisor, Program Lead, Team Leader, Military Rank, Senior Executive	HR system, OPM job code	1	Header Row Label = Grade, Field = GRADE, Source = NFC-PERHIS (USED TO CALCULATE "SupervisorCode"); Header Row Label = Step, Field = STEP, Source = NFC-PERHIS; Header Row Label = Supervisor Code, Field = POSITION-SUPERVISORY-CODE, Source = Calculated from other values; Field = Calculated SupervisorCode, Source = Calculated from other values ("CalculatedCluster," "POSITION-SUPERVISORY-CODE," "WORKING-TITLE-CODE," & "GRADE"); Field = CalculatedBand, Source = Calculated from other values ("CalculatedCluster," "Grade," & "CalculatedSupervisorCode"); Header Row Label = NoPlan, Field = CALCULATED-PLAN-FLAG, Source = CALCULATED from PayPlan;						
Employment Authorities	Management Level (continued)					Header Row Label = JbNm; Field = CALCULATED-JOBNUM, SOURCE = CALCULATED from CALCULATED-CLUSTER and CALCULATED BAND; Header Row Label = PayPlan, Field = PAY-PLAN, Source = NFC-PERHIS (USED TO CALCULATE "NoPlan"); Header Row Label = NoPlan, Field = CALCULATED-PLAN-FLAG, Source = Calculated from other values;						
Employment Authorities	Direct Reports	In combination with Mgt Level -Authority to validate HR data for others, Authoride to override data	By organization code		Multiple	(can CALCULATE from ORG-STRUCTURE-CODE 2nd to 8th levels)						
Employment Authorities	Rating official/ Reviewing official	Persons authorized to validate work assignments, performance appraisals	By organization code	HR system	Multiple	(can CALCULATE from ORG-STRUCTURE-CODE 2nd to 8th levels)						
Personal Characteristics	Citizenship	Used for "NOFORN", Access for treaty participants	US, US Legal Permanent Resident, Canada	CIS, OPM, US Passport Agency	Two?							
Secondary												
Unique Identifier	Unique Identifier	Additional values not easily/consistently available	Signature, Digital signature, Issuer Identification, PIV		Multiple	Header Row Label = Gender, Field = Sex-Code, Source = NFC-PERHIS; Header Row Label = RNO, Field = RNO-CODE, Source = NFC-PERHIS (RNO = race national origin)						

Unique Identifier	Pseudonym		Name before/after divorce, Nickname, Consistent Error		Multiple						
Unique Identifier	Birth date	When linked to name reduces likely individuals to nearly one	12/12/1967	HR system	One						
Employment Activities	Authorized Purpose	Mission established by law (derived from the Constitution)			Multiple	Header Row Label = JbTtl, Field = POSTION-OFFICIAL-TITLE Source = NFD-PERHIS; Header Row Label = PositionNumber, Field = POSITION-NUMBER, Source = NFC-PERHIS;		value = "criminal law enforcement, " "criminal investigation," "civil law enforcement," "administrative law enforcement," "prosecution"	value = "human resources," background investigation," "hiring," "performance evaluation" "discipline," "license investigation," "license review," "benefits granting," "benefits investigation,"		value = "records management inspection" "44 USC 2904," "44 USC 2906"
Employment Activities	Work Assignment	Subject/Topic assignments or Individual matter assignments	Al Queda, Mexican border, Enron investigation	Name of work unit;	Multiple						
Employment Activities	Other Group Membership	May have special access or access limitations	Bargaining unit, Advisory board, Contractor under DD254, Veteran,		Multiple	Header Row Label = BargUnit, Field - BARGAINING-UNIT-STATUS, Soruce = NFC-PERHIS					
Employment Authorities	Special Work Terms	Characteristic of employment relationship	Background investigated, Probation, Weekend shift, Disciplined (security violations)	HR system, Time system	Multiple	Header Row Label = ProbBegin, Field = DATE-PROB-PERIOD-START, Source = NFC-PERHIS; Header Row Label = SupvProbBegin, Field = DATE-SUPV-MGR-PROB-BEGINS, Source = NFC-PERHIS; Header Row Label = ProbEnd, Field = CALCULATED-PROBATION-END-DATE, Source = CALCULATED; Header Row Label = SupvProbEnd, Field = CALCULATED-SUPV-PROBATION-END-DATE, Source = CALCULATED;					
Employment Authorities	Management Level	Authority to validate HR data for others, Authority to override access restriction	Matrix management authority, Component administrator, Programmatic Lead		Multiple						
Employment Authorities	Special Authorities, Special Licenses	Additional values	Master Timekeeper, System Administrator, COTR, Training completed, Licensing Agent								

Personal Characteristics	Skill	Examples:Languages spoken or read other than English, computer skills	French, Arabic, C++, Networking		Multiple							
Personal Characteristics	Skill Level	For each skill a proficiency score	Fluent (s-4, r-4), other proficiency scores									

					T&A	D-Help			HSIN
						Primary			
ients									
Contractors	Litigation	Congress	Audit/ Oversight	Employment Matters	11 Roles= employee, timekeeper, mastertimekeeper, mastertimekeeper restricted, Mastertimekeeper Read only, Administrator, project manager, HR administrator, supervisor, master supervisor restricted, master supervisor global,	Public User	Registered User	Validated Registered User	Close to 500 Communities of Interest (COIs)
Value = [any]	Value = [any]	Value = [any]	Value = [any]		Emp_ID is the primary key in the WebTA system. Source = manual entry		Field = Last Name, Value = [any]; Field = [Middle Name], Value = [any]; Field = First Name, Value = [any]	Field = Last Name, Value = [any]; Field = [Middle Name], Value = [any]; Field = First Name, Value = [any]	HSIN ID can be used for multiple COIs.
	Value = "Department of Justice" or if "Employer Type" value **and** "Authorized Purpose" value are correct	Value = "U.S. Senate" "US House of Representatives"		Value = "Equal Employment Opportunity Commission" "Merit Systems Protection Board" "Office of the Special Counsel" "Federal Labor Relations Authority" "Office of Personnel Management"	Fields = Agency (Agency_ID), Organization (ORG_ID) Roles of Master limit by agency only. Source = Manual Entry				Key to many COIs, For Coast Guard Command Center, Value = Coast Guard, For State and local Itelligence, Value =Any state,local or federal law enforcement organization and contract support.
	Value = "General Counsel" "Counsel" "Cvil Litgation" "Criminal Defense"				ORG_ID link to 2 character code in NFC file, levels include Org_ID, Parent, Agency_ID, UNIT_CODE, PROJ_ID, SUB_PROJ_ID, allows at least four levels				Key attribute for many COIs, such as the Coast Guard Command Center and the NOC

Value = "federal government" LINKED TO Employment Type values	Value = "federal government" LINKED TO Authorized Purpose values or Employer Subgroup Values							Field = [Organization Type], Value = "local," "local region," "state," "state region," "federal," "federal region," "national," "national region," "tribal," "interoperability," "industry-liaison"	Used by some COIs, Example State and local Intelligence COI does not allow private sector (non contract support) or foreign intelligence.
Value = "Contract," "Grant," "Cooperative agreement," "Student Intern" or if AUTHORIZED PURPOSE criteria is met					Only DHS employees in system			Field = Organization, Value = [any?]	Unknown if used
	Value = "attorney" "lawyer" "paralegal"	Value = "Senator" "Senator's staff" "Representative" "Representative's Staff"		Value = "Administrative Law Judge" "Arbitrator"	Position, GRADE. STEP, PAY_PLAN_ID - not used unless change in pay period. TMK_ID creates hierarchy rights toedit time and attendance transaction. SUP_ID creates hierarchy that allows approval activities to be approved. DELEGATED allows delegated authority.		Field = [any equivalent of "job name"], Value = "Emergency Medical Technician," "Fireman," "Police Officer," "Medical" "Emergency Manager" (other disaster management related title) **or** Value = "Mayor," "Governor," (or related staff titles) **or** Authorized Purpose criteria met	Field = [any equivalent of "job name"], Value = "Emergency Medical Technician," "Fireman," "Police Officer," "Medical" "Emergency Manager" (other disaster management related title) **or** Value = "Mayor," "Governor," (or related staff titles) **or** Authorized Purpose criteria met	Core issue for many COIs. Must be Law Enforcment to be in Law Enforcement COI.
					Track STATE, ZIP, CITY, STREET 1, STREET2 - not used for access decisions. Not accomplished by region only supervisor relationship				Regional COIs exist, such as the National Capital Region COI and the Homeland Security task Force - South East COI

						Field = [any equivalent of "domain name"], Value = [any];	Field = ZipCode, Value = [any valid US zip code] (Proxy for geo-coded location); Field = Address. Value = [number, street, city], (Proxy for geocode); Field = telephone number, Value = 10 digit phone number (Area code may be proxy for geocode); Field = email address, Value = [any] (May be proxy for physical location (e.g., governor.state.tx.us);	Field = [any equivalent of "domain name"], Value = ".gov" ".mil" ".us" [Proxy for confirmation of employment at a federal, state, or local government]; Field = ZipCode, Value = [any valid US zip code] (Proxy for geo-coded location); Field = Address. Value = [number, street, city], (Proxy for geocode); Field = telephone number, Value = 10 digit phone number (Area code may be proxy for geocode); Field = email address, Value = [any] (May be proxy for physical location (e.g., governor.state.tx.us);	Can be used as above.
									HSIN is a unclassified system, these should not be used
					TMK_ID establishes Timekeeping role, SUP_ID establishes supervisor role. All others: defined manually:mastertimekeeper, mastertimekeeper restricted, Mastertimekeeper Read only, Administrator, project manager, HR administrator, master supervisor restricted, master supervisor global		Field = [any equivalent of "spacial license'], Value = [any value used in disaster management (e.g., DMV granted emergency license plates or authority to mount emergency lights or state issued license for emergency medical technicians)		Do not know extent of all COIs. LE requires "Sworn" law enforcment defined as having arrest authority

					SUP_ID tracks first level supervisor and can be used to create hierarchy. Not currently vetted outside system Could evaluate SUP_ID against NFC data on supervisory roles				Unsure of use but consistent with the COIs structure
					Manually entered				
					PAY_PLAN_ID used, PROJ_ID and SUB_PROJ_ID also can be used as proxy to obtain this information				
					PAY_PLAN_ID would be a proxy for exemption from Fair Labor Standards Act				Citizenship currently used in State and local Intelligence Community

Value = (any Constitutionally derived federal purpose)	Value = "Administration of Government: Litigation"		Value = "Administration of Government: Audit" "Administration of Government: Oversight"	Value = "Administration of Government: Human Resources: Personnel Matters"			Field = [any equivalent of "authorized purpose" or "mission], Value = "political leadership," "civil service," "emergency management," "homeland security," "first response" **or** Job Name criteria met	Field = [any equivalent of "authorized purpose" or "mission], Value = "political leadership," "civil service," "emergency management," "homeland security," "first response" **or** Job Name criteria met	Many iterations of authorized purpose
									Key attribute for some COIs
									Working group involvement is currently used to creat COIs, We believe that this is a proxy for other attributes but have not fully explored

									Unsure of use