DOT/FAA/TC- 06/09

Federal Aviation Administration
William J. Hughes Technical Center
Atlantic City International Airport, NJ 08405

Human Factors Considerations for Passwords and Other User Identification Techniques

Part 2: Field Study, Results and Analysis

Kenneth R. Allendoerfer, NAS Human Factors Group, ATO-P

Shantanu Pai, L-3 Communications, Titan Corporation

January 2006

Technical Report

U.S. Department of Transportation
Federal Aviation Administration

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof. The United States Government does not endorse products or manufacturers. Trade or manufacturer's names appear herein solely because they are considered essential to the objective of this report. This document does not constitute FAA certification policy. Consult your local FAA aircraft certification office as to its use.

This report is available at the Federal Aviation Administration William J. Hughes Technical Center's full-text technical reports web site: http://actlibrary.tc.faa.gov in Adobe Acrobat portable document format (PDF).

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
DOT/FAA/TC-06/09		

4. Title and Subtitle	5. Report Date
Human Factors Considerations for Passwords and Other User Identification Techniques Part 2: Field Study, Results and Analysis	January 2006
	6. Performing Organization Code AJP-7132

7. Author(s)	8. Performing Organization Report No.
Kenneth Allendoerfer, NAS Human Factors Group Shantanu Pai, L-3 Communications, Titan Corporation	DOT/FAA/TC-06/09

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Federal Aviation Administration NAS Human Factors Group William J. Hughes Technical Center Atlantic City International Airport, NJ 08405	**11. Contract or Grant No.**

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
Federal Aviation Administration Human Factors Research and Engineering Division 800 Independence Ave., S.W. Washington, DC 20591	Technical Report
	14. Sponsoring Agency Code ATO-P

15. Supplementary Notes

16. Abstract

Within the Federal Aviation Administration (FAA) Air Traffic Organization (ATO), Technical Operations (TO) personnel ensure that the systems that make up the National Airspace System (NAS) function safely and effectively. TO personnel manage and maintain more than 44,000 pieces of NAS equipment and systems at over 6,000 facilities and locations. They work at many types of facilities including the National Operations Control Center (NOCC), Operations Control Centers (OCCs), Air Route Traffic Control Centers (ARTCCs), Terminal Radar Approach Control (TRACON) facilities, Air Traffic Control Towers (ATCTs), and Automated Flight Service Stations (AFSSs). The FAA employs a variety of user-identification techniques including knowledge-based techniques, such as passwords, token-based techniques (such as badge readers) to ensure that facilities, equipment, and personnel are secure. In 2004, the Technical Operations Services organization became increasingly concerned about the number of usernames, passwords, and tokens that TO personnel were being expected to use. The NAS Human Factors Group conducted a field study to examine the human factors implications of user-identification techniques currently employed at field sites to prevent unauthorized access to NAS equipment and information technology systems. In this report, we present findings from the field study and provide recommendations that are specific to the TO users, tasks, and environment. These recommendations seek to improve the human factors of user-identification technologies and policies to improve the productivity, workload, and job satisfaction of TO employees.

17. Key Words	18. Distribution Statement
Biometrics, Human Factors, Password, Security, Usability, User-identification Techniques	This document is available to the public through the National Technical Information Service, Springfield, Virginia, 22161

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	38	

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

Table of Contents

Appendixes

List of Illustrations

Figure Page

Tables Page

Executive Summary

Within the Federal Aviation Administration (FAA) Air Traffic Organization (ATO), Technical Operations (TO) personnel ensure that the systems that make up the National Airspace System (NAS) function safely and effectively. TO personnel manage and maintain more than 44,000 pieces of NAS equipment and systems at over 6,000 facilities and locations. The FAA primarily employs knowledge-based user-identification techniques, such as usernames and passwords. The agency also employs token-based techniques, such as badge readers, to ensure that facilities, equipment, and personnel are secure.

In 2004, the Technical Operations Services organization became increasingly concerned about the number of usernames, passwords, and tokens that TO personnel were being expected to manage. The NAS Human Factors Group conducted a field study to examine the human factors implications of user-identification techniques currently employed at field sites to prevent unauthorized access to NAS equipment and information technology systems. Engineering research psychologists from the NAS Human Factors Group visited 13 TO field facilities and conducted structured interviews with 52 employees working in TO. We interviewed participants about their experiences using current user-identification technologies and policies and collected their attitudes toward possible replacement technologies such as biometrics.

Most interviewees reported some difficulties with their usernames and passwords that led them to adopt coping strategies that could reduce overall information security. Interviewees reported problems such as too many passwords to remember, inconsistent password and username rules, systems requiring that passwords change too frequently, systems with too strict password reuse rules, a lack of grace logins, and difficulties resetting forgotten passwords.

Based on the findings of the interviews, we make the following recommendations. First, the agency should explore ways to reduce the number of usernames and passwords TO personnel are required to remember. Second, the agency should develop consistent rules for usernames and passwords across systems. Third, the agency should investigate password management tools. Fourth, FAA systems, especially those with safety or for time-critical functions, should allow at least one grace login where users can access systems even when passwords have expired. Fifth, the agency should provide more information and training to personnel on techniques to build secure passwords that have minimal impact on workload and operations. Sixth, for internal, less-critical systems, the agency should investigate techniques where users can update their passwords themselves. Seventh, the agency should closely investigate the human factors implications of increased use of tokens and implementation of biometrics. Finally, the agency should strive to make the information security requirements of systems match the sensitivity of the information in the system and consider their costs to users in terms of workload and efficient operations.

1. INTRODUCTION

Within the Federal Aviation Administration (FAA) Air Traffic Organization (ATO), Technical Operations (TO)[1] personnel ensure that the systems that make up the National Airspace System (NAS) function safely and effectively. TO personnel maintain current systems and are responsible for the integration of and transition to new systems. They work at many types of facilities including the National Operations Control Center (NOCC), Operations Control Centers (OCCs), Air Route Traffic Control Centers (ARTCCs), Terminal Radar Approach Control (TRACON) facilities, Air Traffic Control Towers (ATCTs), and Automated Flight Service Stations (AFSSs). TO personnel manage and maintain more than 44,000 pieces of equipment and systems at over 6,000 facilities and locations.

The FAA employs a variety of approaches for ensuring that facilities, equipment, and personnel are secure. In this report, we discuss human factors considerations for techniques currently used at FAA field sites to prevent unauthorized access to NAS equipment and FAA administrative information technology (IT) systems. These techniques include knowledge-based techniques, such as usernames and passwords, and token-based techniques, such as badge readers. NAS equipment and IT systems are further protected by property and building security, 24-hour staffing at many FAA operational facilities, and the lack of remote access to many systems.

1.1 Project Rationale

Events such as the attacks of September 11, 2001, the denial-of-service attacks on major corporate websites in 2000, and the rise of spyware and identity theft have raised awareness of information security. In response, government and industry have rapidly implemented new technologies and policies to make it more difficult for intruders to damage IT systems, disrupt services, or obtain sensitive information. Increased information requirements increase the number and complexity of usernames and passwords that users must manage. This increase can affect employee workload and may lead to insecure practices such as writing passwords down. At the same time, technologies such as biometrics have become increasingly affordable and widespread. For these reasons, it is an appropriate time for the FAA to examine how user identification is accomplished in the agency and to recommend changes if needed.

In 2004, the Technical Operations Services organization became concerned about the increasing number of usernames, passwords, and tokens that TO personnel were expected to manage. In response, the FAA Human Factors Research and Engineering Division sponsored a project to examine the human factors implications of user identification techniques in the TO domain. The goal of the project was to develop recommendations for reducing the impact of user identification on employee workload, productivity, and job satisfaction while still meeting strong information security requirements.

---

[1] With the transition to the ATO, most functions once performed by the FAA Airway Facilities organization now fall under ATO Technical Operations Services unit. Other maintenance functions now fall under individual service units. In this report, we use the terms Technical Operations, TechOps, and TO in a general sense to include all FAA personnel engaged in monitoring, controlling, and otherwise maintaining NAS equipment, regardless of their position within the ATO hierarchy.

1.2 Previous Work

In Part 1 of this project, we conducted a review of the human factors literature regarding knowledge-based, token-based, and biometric user identification techniques (Allendoerfer & Pai, 2005). Human factors issues include cognitive issues, such as the number and complexity of passwords that employees must remember. Not surprisingly, the literature shows that people have difficulty remembering many usernames and passwords, especially when they are complex and change frequently. Other human factors issues were social issues, such as the perceived consequences for breaking information security policies. Because nearly all of the existing human factors research in user identification has been conducted in corporate and academic environments, we also analyzed differences between those environments and FAA TO. Finally, we provided general recommendations for improving the human factors of user identification technologies and policies. Our recommendations included reducing the number of logins that employees must remember and providing employees with techniques, such as using mnemonics, that would help them remember their logins more easily.

1.3 Purpose

This technical report provides findings from field visits that the NAS Human Factors Group conducted in March 2005. We interviewed TO personnel about their experiences using current FAA user identification techniques. We identify the cognitive and social pressures TO personnel experience and the coping strategies they adopt to deal with those pressures. We present recommendations that are specific to the TO users, tasks, and working environment. These recommendations seek to improve the implementation of user identification technologies in TO and increase the productivity, workload, and job satisfaction of TO employees.

2. METHOD

Engineering research psychologists (ERPs) from the NAS Human Factors Group visited TO field facilities and conducted structured interviews about current user identification technologies, policies, and practices. The following sections discuss the sites, participants, and data collection techniques we used.

2.1 Sites

We visited the following sites: Cleveland ARTCC, Cleveland TRACON, Atlanta ARTCC, Atlanta TRACON, Atlanta ATCT, the Atlantic Operations Control Center (AOCC), the National Network Control Center (NNCC), Northern Georgia Systems Support Center (SSC), Atlanta Systems Management Office (SMO), Oakland ARTCC, Northern California TRACON, and San Jose ATCT. The sites were selected in coordination with the sponsor to provide a wide sample of TO users, tasks, and working environments.

2.2 Participants

Fifty-two FAA employees working in TO formally participated in the interviews as either individuals or part of a group. The average experience level for the participants was 13.4 years (range: 3-33 years) in the TO environment. The job titles of the participants included Airway Transportation Systems Specialists (ATSSs), NAS Area Specialists (NOMs), NAS Operations Supervisors, system administrators, supervisors, and managers.

In addition, other TO personnel at each facility provided informal information to us because their work schedules prevented them from serving as full participants. We have not included this

information in the formal dataset for the survey, but we have considered it in identifying trends and drawing conclusions.

2.3 Procedure

The Human Factors Coordinator for Technical Operations arranged the field visits and established points of contact (POCs) at each facility. The POCs identified participants at their facilities based on availability and interest. At each facility, the goal was to interview as many participants as possible within the available time. Before answering any interview questions, we briefed the participants on the nature of the study. Each participant signed the statement of ethics and informed consent (Appendix A).

Participants responded to the items on the structured interview questionnaire (Appendix B). First, the ERPs collected demographic information such as job title and experience from each participant, even when the participant was working as part of a group. Second, the participants named every FAA system they work with that employs a user identification technique. Third, participants selected two of these systems to talk about in detail. Finally, participants discussed their opinions and experiences with alternative user identification techniques. Each session lasted approximately one hour.

3. RESULTS FOR FACILITY TYPES AND JOB SERIES

Table 1 presents the total number of different systems employing a user-identification technique reported at each facility type. By interviewing multiple people and by visiting multiple sites, we believe we have identified the majority of the systems in each facility type. However, because participants were asked to name systems, it is possible that they did not recall every system they actually use. Conducting interviews in groups helped alleviate this problem by decreasing the likelihood that a system would be forgotten or overlooked.

Table 1. Systems with User Identification by Facility Type

Facility Type	Number of Systems with User Identification Method
ARTCC	43
ATCT	33
TRACON	23
SMO	23
OCC	18
SSC	9
NNCC	6

Note that individual TO employees do not use every system available at their facility or facility type. The number of systems used by an individual TO employee varies widely by job series and

responsibility level. Even with these caveats, it is clear that most TO personnel are asked to remember a substantial number of usernames and passwords to accomplish their duties.

Table 2 presents the number of systems reported by participants in different TO job series. By interviewing multiple people across multiple facilities, we believe we have identified most of the systems used by job series across the agency. However, for the job series where we were able to interview only a small number of employees, the number of systems used by that series across the FAA will be larger than the number listed here.

Table 2. Number of Systems with User Identification Methods by Job

TO Job Series	# Reported Systems with User identification Method
ATSS	56
Supervisor	30
Manager	25
NAS	22
NOM	12
SDS	7
Computer Specialist	6
Administration Coordinator	3
OCC Specialist	2

There is no individual employee within a job series who uses every system available by that job series. For example, the ATSS job series across TO accesses 56 systems employing a user identification method, but an individual ATSS employee accesses only about 40 of those. The following sections describe four common job profiles in the TO environment and discuss the systems accessed by a typical user in that job series.

3.1 Job Series Profile: Airway Transportation Systems Specialists (ATSSs)

ATSSs install, repair, maintain, operate, and certify the NAS equipment used in ATC. Their duties also include installing and maintaining non-NAS equipment and environmental equipment (e.g., lighting, power, ventilation) in ATC facilities. ATSSs often work out of offices located at or near airports. The equipment they are responsible for is located in and around ATC facilities, on the airport property, and, in the case of surveillance and navigational aids, in remote locations far from airports. ATSSs access multiple systems as part of their duties, each of which typically requires a username and password. Examples of systems accessed by an ATSS include the Maintenance Management System (MMS) used for tracking maintenance events and activities, Lotus Notes for conveying work and maintenance schedules, Joint Acceptance Inspection (JAI)

for facility certification, and Automated Inventory Tracking Systems (AITS) for tracking facility inventory.

The typical ATSS had an average of 13.5 years experience in the TO environment and reported using 40 job-related systems requiring a username and password, 21 of which were NAS systems and 19 were non-NAS. To avoid confusion and lost productivity in recovering forgotten usernames and passwords, a typical ATSS maintained written records of their usernames and passwords in a notebook or personal digital assistant (PDA). The typical ATSS felt that the frequency with which systems request a password change was the most serious problem and suggested moving towards a FAA-wide standard for passwords.

3.2 Job Series Profile: Supervisor for Systems Support Center (SSC)

SSC supervisors are responsible for managing ATSSs, including time and attendance, scheduling, and performance appraisals. SSC supervisors are also responsible for property and financial management for their group and for authorizing training.

SSC supervisors use a variety of systems as part of their duties. For example, the Automated Inventory Tracking System is used to track and maintain property records for a facility. The Integrated Personnel and Payroll System (IPPS) helps the SSC supervisors process time and attendance, personnel actions, and training. The data stored in IPPS includes sensitive personnel information such as Social Security Numbers.

The typical SSC supervisor had 15 years experience in TO and reported using 31 job-related systems requiring a username and password. Many of these systems are accessed from traditional office desktop computers. The typical SSC supervisor reported writing down username and passwords on a piece of paper stored in his or her desk and locked when not in use.

Most usernames and passwords, when forgotten, can be reset by calling the associated SMO and the process may take a few minutes if the appropriate personnel are available. The typical supervisor suggested having a single password for all the intranet based systems.

3.3 Job Series Profile: Communication Navigation and Surveillance (CNS) Supervisor

CNS supervisors are responsible for maintaining the NAS navigation and communication equipment such as radar, instrument landing system (ILS), runway visual range, voice switch and distance measuring equipment. They configure, adapt parameters, and run diagnostics to ensure smooth operation of the NAS navigation and communication equipment. In addition to these, supervisors access other systems such as the Simplified Automated Logging (SAL) which helps them generate, maintain, and review logs of maintenance activities. Username and passwords are the most common form of authentication employed by these systems.

The typical CNS supervisor reported having eight years experience in TO and reported using 17 job-related employing usernames and passwords. The systems are accessed either from an office environment or from the field based on the nature of work. For example, to run diagnostics on an ILS, the supervisor may have to travel to the location where the ILS is installed whereas a maintenance action can be logged using SAL from a back office on a laptop. The typical CNS supervisor reported use of a group password wherever possible so that co-workers could be contacted in the event of a forgotten password. The typical supervisor viewed non-standard password requirements across systems as cumbersome.

3.4 Job Series Profile: NAS Operations Manager (NOM)

NOMs perform a variety of functions directly related to the operation of NAS. They monitor line replacement units, analyze and resolve problems with NAS equipment, initiate action for timely repair and restoration of NAS services and systems, minimize service interruptions by conducting routine diagnostics, and perform service level certifications.

The typical NOM reported accessing 25 systems as part of their duties using a username and password. These included systems that directly support the NOM functions, such as MMS and JAI, and secondary systems such as Labor Distribution Reporting and IPPS, which support time and attendance processing, personnel actions, and training. A forgotten username or password may delay troubleshooting of NAS system problems and may affect NAS operations. The typical NOM reported having forgotten a password when coming back from a vacation or training. Systems requesting a password change at different intervals further complicate the problem. As a coping strategy, the typical NOM maintained records of their usernames and passwords on a personal PDA, a notebook stored in the facility, or in a facility-provided password storage mechanism.

4. USER EXPERIENCES USING KNOWLEDGE-BASED SYSTEMS

The following sections document experiences using usernames and passwords. The first section describes what participants reported during the cognitive and social interviews. It also details the pressures that TO personnel commonly experience in dealing with usernames and passwords. The second section describes the strategies they have adopted to cope with the pressures.

4.1 Pressures

In Part 1 of this project, we discussed cognitive and social pressures that users may face when working with knowledge-based identification techniques (Allendoerfer & Pai, 2005). Cognitive pressures include the number, length, and complexity of passwords and the frequency with which passwords must be changed. Social pressures include issues of accountability, trust, and reputation. The personnel we interviewed during our field visits reported facing many of these pressures.

4.1.1 Inconsistent Rules

Many of the systems we encountered maintain their own rules for password length, complexity, and frequency of change. This makes it more difficult for personnel to manually synchronize their passwords (i.e., use the same password on multiple systems). Some researchers in the information security literature recommend against using the same password on multiple systems (Brown, Bracken, Zoccoli, & Douglous, 2004), but from a human factors perspective, synchronizing passwords reduces users' cognitive pressure and discourages them from adopting more negative coping strategies. Remembering a smaller number of passwords decreases the likelihood that users will write their passwords down or share them with others.

In addition, the rules in many of the systems we encountered were similar but not identical so personnel often confuse them. This makes changing passwords frustrating because users mistakenly try to conform to the rules from another system and their new passwords are rejected. This also increases cognitive pressure because users end up choosing subtly different passwords (e.g., "mypassword1" versus "mypasswd1") across systems because the rules are different. When the items being recalled are very similar to each other, the chance for recalling the wrong one is greatly increased. Participants might be better served by using very different passwords

on each system to reduce the chance for recalling the password for one system when trying to recall the password for another.

Finally, though users normally cannot select their own usernames, inconsistent methods for constructing usernames adds to the cognitive pressure of remembering logins. Usernames tend to be similar but not identical. For example, "doej," "jdoe1234," and "jane.doe" are username styles used in FAA systems. Using a consistent username style across systems would decrease the cognitive pressure on users and discourage them from writing their usernames down.

Inconsistent username and password rules were the most frequently reported problem by the participants. In some ways, this diversity of rules makes the overall system more difficult to hack. A hacker who learns the rules for one system does not necessarily know the rules for others. However, this small benefit does not justify the human factors cost.

4.1.2 Large Number of Logins

As discussed in Part 2 - Section 3, depending on their responsibilities, TO personnel may be responsible for remembering as many as 40 job-related usernames and passwords. Very few people have the ability or motivation to memorize this many logins without writing them down or using a mnemonic. The number of logins places substantial cognitive pressure on TO personnel and encourages them to adopt coping strategies.

4.1.3 Frequency of Change

FAA order 1370.92 (2004b) calls for a maximum password lifespan of 180 days for all but infrequently accessed systems. Most TO systems have a lifespan of either 90 or 180 days. In some cases, the system warns the user before a password is about to expire. Other TO systems allow a small number of grace logins to allow users to change their password. Participants reported that the required rate for most TO systems seemed appropriate but some systems, particularly MMS, required changing the password so frequently that it decreased productivity and job satisfaction.

Requiring users to change passwords frequently increases cognitive pressures and encourages users to adopt coping strategies. Because changing passwords requires effort and time, frequent password changes take time from other important duties. Coupled with strict reuse rules, frequent changes can increase workload and frustration because users must invent new passwords that conform to the complexity requirements and not everyone is able to do this easily (Sasse, Brostoff & Weirich, 2001).

Requiring frequent password changes encourages users to devise ways around the rules, such as changing their current password and immediately changing it back. Requiring frequent changes increases the likelihood that the password will expire while a user is on travel or leave, which can create problems when the user returns home.

4.1.4 Strict Password Reuse Rules

Many systems enforce rules regarding password reuse. That is, when changing a password, users are prevented from using a specified number of previous passwords. In TO, this number varies across systems. In most cases, this number is less than 10, but some systems like Lotus Notes track 50 or more previous passwords.

In addition, some systems require a certain amount of non-overlap between the new password and the previous ones. For example, a common practice is to increment the number in the

password with each change (e.g., “mydog1Spot” to “mydog2Spot”). Some systems require that at least two characters differ (e.g., changing “mydog1Spot” to “my2dog1Spot”).

These rules increase cognitive pressure on users and encourage them to adopt coping strategies like writing passwords down. They also make the process of changing passwords more frustrating because users are prevented from selecting passwords they want and can remember, even if those passwords meet the other complexity requirements.

4.1.5 Infrequent Logins and Travel

Human memory is strongest for information that is used often. Logging into a system frequently improves users’ memories for its usernames and passwords. However, many TO systems, especially those in the NOCs, are logged in at all times and users very seldom enter a username or password. On other systems, personnel login only to conduct periodic maintenance and certification. If the maintenance is required only every month or quarter, and personnel work on varying shifts and schedules, it may be many months between logins for any individual. This increases the likelihood that users will forget their username or password because they do not practice it frequently.

In addition, participants reported that they frequently forgot their logins after returning from an offsite training course, other business travel, or leave. TO personnel regularly attend offsite training courses that last several days and sometimes weeks and this training is sometimes mandatory. While away from their home facilities for any reason, personnel will not normally login to most of their systems, except perhaps Lotus Notes. Lack of use can cause users’ memories for their usernames and passwords to fade, which can lead to problems when the users return to their regular duties. Participants reported that this was especially true when they had changed the password shortly before leaving for training or leave. In psychological terms, the new password had not been strongly encoded in the users’ memories when they left the facility and degraded even more quickly due the lack of use while on travel.

Finally, participants reported that passwords sometimes expired while they were away from the facility. This created problems when they returned, especially for systems without a grace period.

4.1.6 Difficulties Resetting Forgotten Passwords

Obtaining a new password or having one reset is normally straightforward, provided the user knows the process and the right person to contact. Participants did not always give consistent answers about how to have a password reset for a particular system suggesting that their knowledge of the process is often inaccurate. In addition, participants reported that password resets occurred quickly when the person responsible was available, but when the password is forgotten outside weekday working hours, the delay could be hours or days.

All TO systems that require frequent password changes allow users to change passwords without assistance when the passwords expire. A call to a system administrator is not necessary, so long as the user remembers his or her current password. However, users who forget their usernames or passwords must contact a supervisor or system administrator. If the appropriate person is unavailable, users may have to wait for a long time to login. This could have consequences during safety- or time-critical situations where a password has expired and cannot be reset.

Many commercial websites allow users to reset passwords themselves by requiring the user to provide some other information, such as a mother’s maiden name, and then a new reset password

is e-mailed to the user. Another mechanism is for the website to allow users to write hints for themselves which might contain abbreviations or explanations of the password in case it is forgotten. Only one FAA system, Lotus Notes webmail, allows users to reset their own passwords. It does this by e-mailing the user a new, reset password to an established FAA e-mail account. However, the implementation is ineffectual because Lotus Notes e-mails the reset password to the user's FAA e-mail address, which the user cannot access because he or she has forgotten the password to get into e-mail. This feature is effective only if the user has access to the desktop version of Lotus Notes in addition to Lotus Notes webmail, which is not normally true on travel or at locations distant from the user's home facility where Lotus Notes webmail is typically used. As we learned during our site visits, many TO personnel share administrative computers and only have access to the webmail version.

4.2 Coping Strategies

The cognitive and social pressures encourage TO personnel to adopt coping strategies for dealing with their many passwords and usernames. Not every coping strategy is negative. In fact, some are creative solutions to difficult problems and could benefit others if the strategies were communicated widely.

4.2.1 Group Logins

About 41% of facilities reported using group logins making them the most common coping strategy we encountered. In this strategy, employees with similar responsibilities share a single username and password. Personnel reported having ad hoc procedures for alerting their co-workers when the group password changes. These procedures include recording the change in a maintenance logs or providing it during relief briefings. Personnel also reported recording group passwords in locations known to the group members. They also reported e-mailing passwords to the members of their work groups.

Another technique is for the group to agree upon a password change technique or system. If a group member misses the announcement of the change, the group member can still probably "hack" the new password by applying the established technique. For example, the group might agree to always change the last two letters of the password to the next letter in the alphabet. If a user cannot log in because the password was changed overnight, the user can determine the new password by applying the known rule to the original password.

4.2.2 24-Hour Login

The operational needs of the NAS require certain systems to be operational and logged in at all times. This has two human factors benefits. First, at a shift change, personnel do not need to logout and login to multiple systems. If logging out and logging in were required for the numerous systems at the SOCs in ARTCCs and large TRACONs, shift changes would take much longer than they do now and would distract from other information in relief briefings. Second, if most systems are logged in at all times, it effectively reduces the number of passwords that a person must remember individually. In this case, there is very little chance that a forgotten password will affect NAS operations because users must login only after reboots. In the rare instance that a password is needed, such as after a system reboot or a software update, the user can find the username and password in a notebook or other known location.

4.2.3 Writing Passwords Down

Forty-two percent of participants reported that they recorded their usernames and passwords on paper or in an electronic device. Some participants reported keeping their lists in locked desk drawers in their offices; others kept them on their person in their wallets, day planners, briefcases, or attached to their FAA badges. In cases where multiple users shared one login, the group usernames and passwords were typically stored in binders or manuals or were written in known locations in the group's common work area. One facility reported that they maintained written records of all root passwords in a locked safe inside the facility that could be accessed during emergencies by managers who knew the combinations.

It should be noted that logins recorded and stored in the operational facility are protected by, at minimum, by building security, room access control, and 24-hour staffing. These measures provide a level of protection from external intruders. However, internal intruders would probably find it easy to obtain usernames and passwords for at least some systems in each facility. Usernames and passwords recorded in a manner that is frequently removed from the facility, such as a briefcase or a planner, has minimal protection against loss or theft.

4.2.4 Password Management Tools

Several facilities have developed their own local practices for storing and protecting passwords. Some personnel store their passwords on their PDAs or other electronic devices like digital watches or cell phones. At one facility, a TO employee used a PDA equipped with a fingerprint scanner. He used the scanner to protect his list of job-related and personal passwords. The additional security of the biometric device allowed the employee to take his passwords with him to off-site locations where he needed to access systems as part of his duties. He purchased the PDA with his own money and selected one with biometric security on his own initiative.

Another facility operated software known as the Password Keeper (Braun, 2005) on a common personal computer (PC). The software itself was password-protected and the PC was only accessible in the SOC, which is staffed at all times. Employees assigned to the SOC with similar responsibilities and authorization levels shared group passwords for many systems. The local practice for using Password Keeper was that the first authorized employee to see a request for a password change would update the password, record the new password in Password Keeper, and notify all of his or her co-workers.

These technologies normally encrypt the file containing the stored passwords and access to the file is often protected by its own password or other authentication technique. In the case of a group password management tool, the login for the tool is known to all the authorized users and changes are distributed by word of mouth or e-mail.

4.2.5 Memory Techniques and Mnemonics

Nineteen percent of the participants reported deriving their passwords from names of their children, pets, hobbies, vacation spots, or their favorite shopping items. Eleven percent of participants reported incrementing their passwords (i.e., each subsequent password increments the digits of the previous).

Participants also reported using systems like always changing the numbers in the password to reflect the current month or season. No participants reported using more advanced mnemonics like phrases, rhyming, or visualization, despite their demonstrated ability to improve memory (Allendoerfer & Pai, 2005). We suspect this is because TO personnel have not received training

about these techniques. The techniques can be difficult to learn, and they may seem like overkill.

5. USER EXPERIENCES USING TOKEN-BASED SYSTEMS

Twenty-three percent of the participants had used token-based user-identification systems for gaining access to facilities, doors, and IT systems. The token systems in use fall into three categories: proximity cards, smartcards, and password generator tokens. Thirty-three percent of the participants using a token reported having forgotten it at home at least once. No instances of a lost or stolen token were reported. Participants reported a lost token could be replaced locally (and the old one deactivated) in most cases.

5.1 Proximity Cards

Proximity cards are used mainly for door access. A proximity card emits a radio signal that is received by a sensor near the door. The maximum distance between the card and the sensor varies with technology. The systems we saw in the field visits required users to be within a few feet of the sensor. The employees normally wore their cards on lanyards around their necks or clipped to their belts.

Seventy-one percent of the participants reported that they had forgotten their door access card at least once. They reported, in these cases, they could contact a supervisor or co-worker who would let them into the facility. Some participants reported having physical keys for doors as backup in case they forgot their proximity card or the sensor malfunctioned.

5.2 Smartcards

Smartcards are plastic cards containing small memory chips. TO field technicians use smartcards to access their laptops, which are outfitted with smartcard readers. Personnel are assigned individual smartcards. If users lose their smartcards or the smartcards stop functioning, it must be brought or mailed to the SMO. The laptop is inaccessible until a new smartcard arrives. If the problem occurs outside weekday business hours, there is no way for the field technician to use the laptop or reset the password.

Participants reported that they normally store their smartcards in the same bag as their laptop. If a laptop were lost or stolen, the accompanying smartcard probably also would be lost because users often store the cards with their laptop cases. In general, the participants did not believe that the smartcards provided any additional security over the other multiple usernames and passwords already required for the laptop. The participants did believe that the smartcards significantly increase frustration because the smartcards and associated logins slow down the laptop and delay the user. Participants also reported that the smartcard readers in their laptops were not reliable.

5.3 Password Generator Tokens

This technology is a combination of knowledge- and token-based techniques. Some TO system administrators have these devices for accessing servers from outside the facility. These devices are not tokens in the traditional sense in that the token itself is not used for access. Rather, the devices generate long random series of numbers every minute. If the user wishes to login to a protected system, he or she enters the number appearing on the token during that minute. TO personnel who have used this technology seem to like it and reported that it was helpful because they no longer needed to remember long passwords that changed frequently. However, the

technology was only available on a small number of TO systems and was more expensive to administer than traditional knowledge- or token-based techniques.

6. USER ATTITUDES TOWARD BIOMETRIC SYSTEMS

No FAA system we encountered used a biometric technology. Fifteen percent of the participants reported using some form of biometric system outside of their job. In one case, a participant had a fingerprint scanner on his personal PDA that he used to store his usernames and passwords.

All participants reported that they would be comfortable using a biometric system after a short period of adjustment. Some said that they might feel uncomfortable at first but all predicted that they would quickly become accustomed to the biometrics. Most participants preferred a fingerprint scan over other biometric technologies.

The participants did raise a number of concerns that would need to be addressed before a biometric system could be implemented in TO. Some of these concerns are related to the usability of the biometric technology, especially by people with disabilities or characteristics different from the perceived norm. Other concerns relate to broader issues of personal privacy and identity theft. These concerns, raised by the participants, are listed and categorized below.

Technical and Implementation Issues

1. How reliable and accurate is the technology?
2. How is the technology maintained and serviced?
3. How will users be trained on the technology?
4. Will a backup system or process be available if the technology fails?
5. Is biometric technology cost-effective, especially compared to token-based systems?

Usability and Accessibility Issues

1. How quickly does the technology verify the user's identity? Users want to sit down at the computer and begin working as quickly as possible.
2. How often must the user login? Touching the sensor once when logging in would be acceptable; touching the sensor every time an application is launched would not.
3. Will the technology work in environments with limited space? The biometric sensors must be small enough to fit on crowded desks and work areas.
4. All biometric systems need to account for physical changes associated with ageing. Voice and facial recognition systems are especially problematic in this area.
5. Fingerprint and hand geometry scanners would need to account for TO jobs where technicians' hands can be dirty or where gloves are required.
6. Alternatives to the biometric technology would be necessary to assist employees with short-term injuries that would interfere with the system. For example, an employee recovering from wrist surgery would have difficulty using a hand geometry scanner or an employee with a cut on the thumb may need to have a fingerprint scanner reset to accept a different finger.
7. Alternatives to biometrics would be necessary to accommodate employees with disabilities that hinder or prevent them from providing the biometric characteristic. For

example, employees who have limited use of their hands would have difficulty providing a fingerprint or hand geometry scan.

Privacy Issues

1. Fingerprints in particular are associated with crime and may make some people feel tracked and watched. However, as Federal employees, TO personnel have already provided the government with their fingerprints. Nearly all participants reported that they would not be uncomfortable providing fingerprints for user identification.
2. How is the database containing the biometric information secured? If that database is compromised, an identify thief could have access to employees' fingerprints or other data. Unlike passwords and tokens, biometric data cannot be reset if stolen. That is, if a thief obtains employees' fingerprint data, the employees cannot be issued new fingerprints. As biometrics become more common, compromised biometric data could lead to problems in employees' outside lives.

7. RECOMMENDATIONS

In Part 1-Section 6 (p. 20), we provided a number of general recommendations for improving the usability of passwords, tokens, and other user identification systems (Allendoerfer & Pai, 2005). In general, we found that these general recommendations were supported by our findings from the field sites. In the sections that follow, we provide more specific recommendations tailored for TO that resulted from our field visits.

7.1 Reduce Number of Passwords

We recommend that the FAA adopt policies aimed at reducing the number of passwords that TO personnel must remember. For some systems used by TO, such as the desktop version of Lotus Notes/Microsoft Windows and MMS/Event Manager, logins are already synchronized and participants found this very helpful. Allowing passwords to be synchronized across more systems or providing a centralized user identification service, commonly known as "single sign-on," would meaningfully reduce the users' difficulty recalling passwords. It would also discourage coping strategies like writing the passwords down. Furthermore, reducing the number of passwords would reduce costs and workload associated with resetting forgotten passwords.

Many of the systems used by TO personnel are administrative and use standard configurations, such as a desktop PC with Microsoft Windows. Administrative systems are typically located in traditional office environments. These factors make it more feasible for the FAA to provide single sign-on for administrative systems than for NAS systems, which carry special operational and technical considerations. Even if NAS equipment could not be included, a single sign-on capability for administrative systems would provide significant benefit to TO personnel.

7.2 Develop Consistent Rules Across Systems

We recommend that the FAA increase enforcement of existing policies regarding password length, complexity, frequency of change, and reuse. These policies can be found in documents such as the Protection Profiles issued by the Chief Information Officer (FAA, 2004a) and FAA order 1370.92 (FAA, 2004b). Currently, there is very little consistency across TO systems. This is an information security issue in that systems may not be using adequate security measures. This is also a human factors issue because it prevents users from adopting the same password on

multiple systems. This increases the likelihood that users will forget passwords and that they will adopt negative coping strategies like writing passwords down.

We recommend that all TO systems explicitly provide the rules for passwords on the page, window, or screen where passwords are changed. This will reduce the effort and frustration that users feel when updating their passwords. For example, the desktop version of Lotus Notes explicitly informs users of the rules for passwords on the window where passwords are changed (see Figure 1). This helps users remember complicated rules and encourages better password practices.

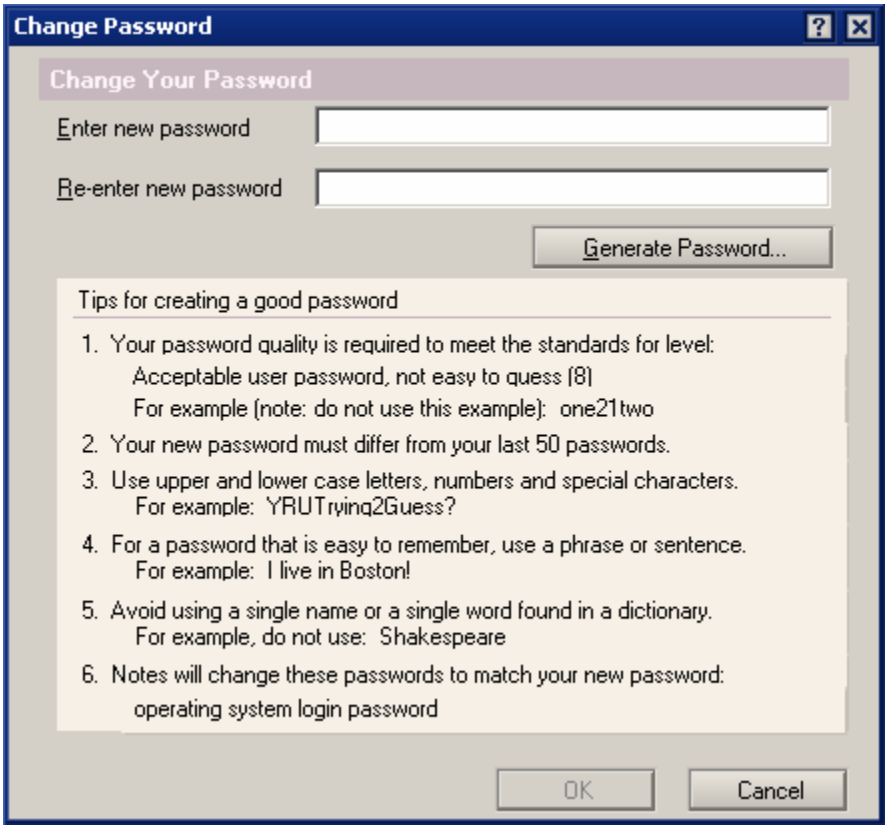

Figure 1. Lotus Notes Change Password dialog box.

7.3 Password Management Tools

We recommend that the FAA provide tools for storing and protecting passwords. FAA order 1370.92 (FAA, 2004b) allows users to store passwords electronically as long as they are protected by digital encryption. A number of TO personnel used their personal PDAs and other electronic devices to store their usernames passwords. The fact that employees are purchasing and using personal password management tools and taking initiative to purchase ones with encryption and information security measures, indicates that there is a need for a password management solution for some TO employees. When such a demonstrated need exists, it would be preferable for the FAA to provide the equipment rather than relying on the initiative and efforts of individual employees. Employees may not make use of the technology due to its expense and may choose a less secure method (e.g., sticky notes) instead. Alternately,

employees may purchase password management equipment but without adequate security measures.

One facility maintained software called Password Keeper (Braun, 2005) which employees at the SOC used to track their group passwords on a standalone PC in the common work area. Password Keeper stores usernames and passwords in a strongly encrypted file. Accessing Password Keeper requires its own password. Participants at this facility reported that they liked the product and that it helped them manage their passwords more effectively. Similar software is available commercially as Password Vault (CamTech2000, 2005) and Norton Password Manager (Symantec, 2004), and as open source as Password Safe (Shapiro, 2005). We recommend that the FAA evaluate this type of product and make it available for wider distribution to facilities with accompanying policy guidelines for effective use.

7.4 Grace Logins and Warnings

Systems that require users to change passwords normally provide a warning that the user's password is about to expire. These warnings are useful but participants reported that they were sometimes too aggressive and too frequent. This gives users the impression that they are constantly changing their passwords. For example, Lotus Notes starts reminding users 21 days beforehand that their passwords will expire. Because Lotus Notes passwords must be changed every 90 days, users are being reminded to change their passwords nearly 25% of the time they use Lotus Notes. This is annoying to users, adds more user actions to every login, and makes it easy to ignore because it occurs so often that it ceases to be noteworthy.

More importantly, many NAS systems are time and safety critical. It would be adverse to operations if a TO user needed to access a system in a time-critical situation only to find that his or her password had expired and needed to be reset.

We recommend that all FAA systems, especially those that are safety or time-critical, provide at least one grace login so that users can enter a new password once the old one has expired. Allowing a grace login will reduce workload for system administrators and reduce user frustration.

7.5 Training

When a system is installed, TO personnel typically receive some sort of training on maintaining passwords for that system. They also receive periodic security training and awareness programs such as the Security Awareness Virtual Initiative (SAVI). However, this training does not focus on the human factors aspects of information security and does not provide useful advice on techniques for remembering passwords.

In the 1990s, the FAA William J. Hughes Technical Center published guidelines for air traffic controllers on ways to improve their memories (Stein, 1994). This guide is written in an informal style and is provides very practical advice. We recommend that the FAA sponsor a similar guide for informing TO personnel on methods for creating passwords that are easy to remember but hard to guess. Some of these methods are discussed in Part 1-Section 6.4 (Allendoerfer & Pai, 2005).

7.6 Mechanisms for Automatically Resetting Passwords

Many commercial websites provide ways for users to obtain new passwords when their passwords are forgotten or lost. Typically, users must provide an answer to a challenge question

(e.g., mother's maiden name). If the challenge question is answered correctly, the system resets the user's password and e-mails the new password to the user with an expectation that the user will immediately change the reset password. We recommend that TO systems, especially administrative systems available on the FAA intranet, provide similar functionality. This will allow users who forget their passwords to obtain new passwords more quickly and will allow users, especially those working during non-business hours, to reset forgotten passwords. Obviously, this technique would not provide sufficient security for all TO systems, but it should be available when appropriate.

7.7 Tokens

The TO personnel we interviewed were nearly universal in their dislike of the smartcards currently in use on their laptops. Some of this reaction results from the unreliability of the current smartcard readers. Most of the reaction, however, comes from a belief that the smartcards and the associated logins create unnecessary work and provide little benefit in increasing security. This suggests that the utility and benefits of the smartcard technology and the associated costs on employee productivity were not adequately considered at the time of implementation.

However, participants were supportive of the concept of token-based user-identification in general. This may be due to their positive experiences with current access control cards. The participants responded that using a token-based technique, such as a proximity card, *in place* of existing knowledge-based techniques would be an improvement that would reduce their workload. However, the participants cautioned that using a token based technique *in addition* to existing knowledge-based techniques would make their jobs more difficult. The participants also responded that it would be acceptable if the token-based system required a "swipe" only when the user is beginning a shift or returning from a break. Participants responded that they would find it unacceptable to be required to swipe the token frequently, such as when launching individual applications.

We recommend that the FAA increase the use of token-based authentication technology in IT systems. If implemented, we recommend that the tokens replace existing knowledge-based techniques and recommend against adding tokens on top of existing usernames and passwords. In the case of the current laptop smartcards, the tokens increase the effort and time required to login to the laptop, which increased frustration and decreased employee productivity. A successful implementation of token technology is feasible but it must not increase, and should preferably reduce, the number of usernames and passwords that personnel are expected to manage.

7.8 Biometrics

The participants expressed cautious but generally positive attitudes toward biometrics. Some said that they were comfortable with the idea, especially with fingerprint scanners, because the FAA already has records of their fingerprints. Personnel were more cautious about iris scanners and other less common technologies but even these were not viewed to be much of a problem, provided the issues discussed in Part 2-Section 6 are addressed.

We recommend that the FAA research the human factors and usability implications of biometric technology further, especially fingerprint scanners. We recommend that the FAA select a test site and deploy a biometric system as a usability field test. This way, the agency can examine

implementation, technical, acceptance, and human factors issues upfront. Human factors professionals should be involved with the field test to measure how the technology affects productivity and job satisfaction. This testing could be combined with other technical testing of the technology.

7.9 Security Requirements Should Relate to Risk and Address Human Factors Costs

In our opinion, it is not realistic to say that every system used by TO personnel must maintain the highest levels of information security at all times. Practices in the field will continue to vary based on local priorities, procedures, staffing, training, and equipment. Not every TO system currently containing sensitive information is strongly protected nor does every system that is currently strongly protected contain sensitive information. Some operational NAS systems have group passwords that never change while some TO administrative systems require usernames and complex passwords that change frequently. This creates productivity and job satisfaction issues by unnecessarily increasing the number of passwords that users must remember without increasing security for critical systems.

We recommend that all TO systems be examined to ensure that the user identification technology and requirements being applied to each are appropriate given

1. the overall risk profile of the system,
2. the level of sensitivity of the data contained in the system, and
3. the effects of user-identification technology and policies on employee productivity.

Many TO systems are not accessible over the internet and are accessible only in locked rooms in 24-hour guarded facilities. In these cases, the review should address whether the associated human factors costs of managing complex passwords or tokens for these systems are justified. Increases in user identification should be implemented where the risk profile warrants but these changes should mitigate, wherever possible, the human factors costs. For example, additional password requirements could be placed on remote navigation systems, but the agency could provide PDAs with encrypted password storage to help authorized personnel manage the new passwords better. Note too that sensitivity is not limited to NAS systems. Personal information like Social Security Numbers and performance reviews are extremely sensitive and need to be protected at a high level.

8. CONCLUSION

We believe that the current approach to user identification in TO creates numerous human factors problems and warrants several changes. TO personnel must remember so many different usernames and passwords and follow so many different rules for password complexity that they are adopting coping strategies for remembering and managing their logins, many of them negative. By following the recommendations contained in Part 1 (Allendoerfer & Pai, 2005) and this part of the report, we believe that TO can substantially improve the usability of user identification in its systems. We believe that doing so will increase employee productivity and improve the overall security of TO systems.

References

Allendoerfer, K. R., & Pai, S. (2005). *Human factors considerations for passwords and other user identification techniques part 1: Literature review & analysis* (DOT/FAA/CT-05/20). Atlantic City International Airport, NJ: Federal Aviation Administration, William J. Hughes Technical Center.

Braun, G. (2005). Password keeper [Computer Software]. Retrieved from http://www.gregorybraun.com/PassKeep.html

Brown, A., Bracken, E., Zoccoli, S., & Douglous, K. (2004). Generating and remembering passwords. *Applied Cognitive Psychology, 18,* 641-651.

CamTech 2000. (2005). Password Vault [Computer Software]. Retrieved from http://camtech2000.net/Pages/PassVault.html

Federal Aviation Administration. (2004a). *FAA High Risk NAS WAN Security Function Protection Profile* (Document Control Number: AIO-4-PP-HRNASWAN1.0). Washington, DC: Author.

Federal Aviation Administration. (2004b). *Password and PIN management* (Order 1370.92). Washington, DC: Author.

Federal Information Processing Standards Publication 112. (1985). Password usage. Retrieved July 20, 2005, from http://www.itl.nist.gov/fipspubs/fip112.htm

Sasse, M., Brostoff, S., & Weirich, D. (2001). Transforming the 'Weakest Link' - A human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*, 122-131.

Shapiro, R. (2005). Password Safe [Computer Software]. Retrieved from http://passwordsafe.sourceforge.net/

Stein, E. S. (1994). *The controller memory guide: Concepts from the field* (DOT/FAA/CT-TN94/28). Atlantic City International Airport, NJ: Federal Aviation Administration, William J. Hughes Technical Center.

Symantec. (2004). Norton Password Manager 2004 [Computer Software]. Retrieved from http://www.symantec.com/passwordmanager/

Acronyms

AFSS	Automated Flight Service Station
AITS	Automated Inventory Tracking System
AOCC	Atlantic Operations Control Center
ARTCC	Air Route Traffic Control Center
ATCT	Air Traffic Control Tower
ATO	Air Traffic Organization
ATSS	Airway Transportation Systems Specialist
ERP	Engineering Research Psychologist
FAA	Federal Aviation Administration
ILS	Instrument Landing System
IPPS	Integrated Personnel and Payroll System
IT	Information Technology
MMS	Maintenance Management System
NAS	National Airspace System
NNCC	National Network Control Center
NOCC	National Operations Control Centers
NOM	NAS Operations Manager
OCCs	Operations Control Centers
PC	Personal Computer
PDA	Personal Digital Assistant
POC	Point of Contact
SAL	Simplified Automated Logging
SAVI	Security Awareness Virtual Initiative
SMO	Systems Management Office
SSC	Systems Support Center
TO	Technical Operations
TRACON	Terminal Radar Approach Control

Appendix A

Statement of Participant Confidentiality and Informed Consent

Statement of Ethics and Informed Consent

Nature and Purpose of the Event

The purpose of this questionnaire is to collect feedback about your experience using authentication systems such as passwords and ID badges.

Participant Description

AF specialists and the managers will form the study population. We intend to interview 4-8 participants per facility from 12 different FAA facilities. Both new and experienced personnel will be interviewed. Our goal is to recruit participants so that different areas within AF (e.g., communications, navigation, surveillance) are well represented.

Experimental Procedures

Following a briefing on the purpose of our study, a human factors engineer from the NAS Human Factors Group at the William J. Hughes Technical Center you will interview you. Listen carefully to each item as it is read to you. Give the interviewer the most accurate and complete response you can. The interview will last about 1 hour.

Once all interviews are complete, you are invited to participate in a group caucus with other AF personnel from your facility who have also participated in the study. The group caucus is intended to refine, clarify, and consolidate issues identified during the one-on-one interviews. The group caucus will last about 2 hours.

Data Collection Methods

Your responses will be collected through the interviews and the group caucus.

Discomforts and Risks

The approximate time required to complete each interview is 1 hour. Questions in the interview will ask you to describe incidents when you or forgot your password, lost your ID badge or otherwise had a problem with an authentication system. Questions in the interview will ask you to describe incidents where you may not have followed FAA policies or best practices with regard to an authentication system. Discussing topics such as these may cause you some discomfort or embarrassment. All your responses will be collected anonymously and no record will connect individuals to responses. Your responses will be used in reports or briefing and will not be released to any person or organization without your expressed permission.

Benefits

There is no direct benefit for your participation. In general, you may expect an eventual benefit of an improved authentication systems or policies as a result of the research.

Participant's Responsibilities

You will be required to respond to the interview questions to the best of your ability. It is expected that you will not discuss the content of the interview with anyone. It is also expected that you will keep confidential any information about the other participants' opinions and experiences that you may learn during the group caucus.

Participant's Assurances

Human Factors Engineers from the NAS Human Factors Branch of the William J. Hughes Technical Center maintain strict standards regarding participant confidentiality and informed consent in all our research. Our standards are based on the *Ethical Principles in the Conduct of Research with Human Participants* by the American Psychological Association and are structured around four main principles

Your participation in this study is completely voluntary. You may withdraw from this study at any time without consequence. If you feel you must withdraw for whatever reason, please inform us immediately. In addition, the human factors engineers may terminate your participation if they feel this to be in your best interest.

Your responses will be identified by a code known only to you and the human factors engineers conducting the study. Your identity will be kept separate from the data you provide. To facilitate this, please do not write your name or any other identifying marks on the questionnaires. Please do not share your participant code with anyone other than the human factors engineers. Your name will not be associated with any data contained in any report or briefing.

The raw data collected in this assessment will become the property of the NAS Human Factors Group. The raw data will be analyzed by specialists from this organization and its contractor employees. The raw data will not be made available to any other person or organization without your expressed permission. The aggregate data from this assessment will be presented in briefings and reports written by the NAS Human Factors Group. Aggregate data will take the form of consolidated comments in which all identifying information has been removed and the wording has been rephrased to obscure the identity of the participant or participants who made the comment. Aggregate data may also take the form of averages, standard deviations, and other statistics.

If you any have questions about this study or need to report any adverse conditions you may contact the human factors engineers. You may also contact Dr. Earl Stein (609) 485-6389, the NAS Human Factors Group Manager, NAS Human Factors Group at any time with questions or concerns.

I have read this consent document. I understand its contents, and I freely consent to participate in this study under the conditions described. I have received a copy of this consent form.

Research Participant: _____ Date: _____

Investigator: _____ Date: _____

Witness: _____ Date: _____

Appendix B

Password Alternatives for Airway Facility Systems

Questionnaire

Purpose:

The following questions are designed to collect feedback on your experience using authentication systems.

Instructions for Participant:

Listen carefully to each item as it is read to you. Give the researcher the most accurate and complete response you can. Please be aware that the interviewer may not know all the terms or concepts that you may describe. If you do not wish to answer a question, for whatever reason, please say so to the interviewer. If you have any questions, or do not understand an item, please inform the interviewer. The information you provide will be anonymous and kept strictly confidential as described on the Informed Consent sheet. Thank you for your participation.

Instructions for Interviewer:

Read each item to the participant slowly and carefully. When the item offers choices, read the choices to the participant and check the box corresponding to their response. Make notes and record their response in the comment area associated with each item.

BACKGROUND & INTRODUCTION

Participant Code: _____ Interviewer Code: _____

Date: _____ Facility: _____

1. What is your current job title? _____
2. How long have you worked in airway facilities/technical operations? _____ years
3. How many AF specialists currently work at your current facility? _____
4. How many AF specialists normally work during a shift? _____
5. How many system administration personnel are available at any given time? _____
6. How many different operational systems (e.g., ATC automation systems, communications, navigation, surveillance) do you access to accomplish your regular duties? _____
7. Of these, how many have unique username and password combinations that you have to remember? _____
8. How many different non-operational systems (e.g., time and attendance, travel manager) do you access to accomplish your regular duties? _____
9. Of these, how many have unique username and password combinations that you have to remember? _____
10. Because we cannot cover every system in detail during this interview, we would like to focus on the systems that you feel are most important to your duties. This may be a system that you access often, a system that contains critical data, or a system that you feel does authentication especially well or poorly. Feel free to discuss operational or non-operational systems.

    Please name 2 systems (1 operational and 1 non-operational) that you access which you feel are the most important ones. You will have a chance to comment on other systems later in the interview.

    SYSTEM 1: _____

    SYSTEM 2: _____

Participant Code: _____

REPEAT FOR SYSTEMS 1 and 2

11. What tasks do you normally accomplish when you access **SYSTEM 1**?

_____

_____

_____

12. What is the environment like where you access **SYSTEM 1**?

- ☐ Office, cube
- ☐ Equipment room
- ☐ Operations floor
- ☐ Outdoors (sunlight, weather)
- ☐ Noisy environment
- ☐ Restricted physical space
- ☐ Unusual working position (e.g., lying on back, using ladder)
- ☐ Other attributes worth noting:

13. How often do you normally access **SYSTEM 1**?

- ☐ Multiple times a day
- ☐ Every _____ days, as required by maintenance procedures
- ☐ Only when a problem arises, approximately every _____ days
- ☐ Other (please explain) _____

Participant Code: _____

14. Which of the following represents the security process employed to access **SYSTEM 1**? Each of the security process may use one or more of the following: badge (B), smart card (S), key (K), username (U), password (P), personal identification number (PIN), fingerprint (F), iris (I), hand geometry (H), voice recognition (V), or a facial recognition (FA). Next to each applicable security process use the abbreviations in brackets to indicate which system is employed in the security process.

    - ☐ Facility/site security _____
    - ☐ Room access security _____
    - ☐ Locked cabinet _____
    - ☐ Information security _____
    - ☐ Staffed security _____
    - ☐ Surveillance cameras _____
    - ☐ Other _____

15. If you were unable to access **SYSTEM 1** due to an authentication problem, even for a few minutes, describe what consequences, if any, the operation might experience.

If your answer to question 15 is:

1. Badge, smart card or key, skip to token-based systems (Question 27).
2. Username, password, or PIN, skip to knowledge-based systems (Question 17).
3. Fingerprint, iris, hand geometry, voice recognition, facial recognition, skip to biometric systems (Question 34).

Also, some systems may use a combination of methods or a method not listed in Question 15. In this case, complete every appropriate section.

Participant Code: _____

Knowledge-Based (Password) Method

16. Do have your own individual password or do other users with similar responsibilities share one? For example, there might be one AF password to access the system that is known to all the certified technicians but is not known to AT.

17. Are you assigned your username/password or can you choose your own?

18. If you are allowed to choose your own, please describe any guidelines or requirements that **SYSTEM 1** has, such as a required length or the use of special characters or capitalizations, for choosing your password.

19. Did you receive any training or information on "best practices" for choosing a password for **SYSTEM 1**?

20. How often does **SYSTEM 1** require you to change your password?

- ☐ Never
- ☐ Once a day
- ☐ Once a week
- ☐ Once a month
- ☐ Every _____ days
- ☐ Other _____

21. When changing your password, does **SYSTEM 1** allow you to choose a similar password with minor changes or do you have to construct a new password each time?

Participant Code: _____

22. Can you describe an occasion(s) when you forgot your username or password for **SYSTEM 1**?

23. If you forget your password for **SYSTEM 1**, how do you reset it or obtain a new one? How long does this process normally take?

24. Is there a way to reset the password yourself, such as by answering a secret question? If yes, how?

25. Do you use any kind of memory aids for recalling your username/password for **SYSTEM 1**?

Token-Based (Badge) Method

26. Do you have your own individual tokens or do other users with similar responsibilities share one? For example, there might be one key to access the equipment panel that all the technicians use.

27. Did you receive any training or information on "best practices" for handling your token for **SYSTEM 1**?

28. How often does **SYSTEM 1** require you to update your token?

- ☐ Never
- ☐ Once a day
- ☐ Once a week
- ☐ Once a month
- ☐ Every _____ days
- ☐ Other _____

Participant Code: _____

29. Can you describe an occasion(s) when you forgot or misplaced your token for **SYSTEM 1**?

30. If you lose or misplace your token for **SYSTEM 1**, how do you get a new or temporary one? Who do you contact and how long does this process take?

31. Do you use any kind of memory aids for remembering or keeping track of your token for **SYSTEM 1**?

32. Can you describe an occasion when the token-reader malfunctioned or was unavailable due to a technical problem? How did you access the system?

Biometric Method

A biometric identification system uses a pattern recognition system to make a personal identification by verifying the authenticity of a specific physiological characteristic, such as fingerprint, retinal pattern, iris, face, wrist vein, hand geometry, or a behavioral characteristic, such as handwriting, signature, or speech. The following questions are intended to collect your views on biometric authentication system should such a system be implemented.

33. Outside of work, have you used a biometric system before?

    ☐ Yes

    ☐ No

34. Biometric systems sometimes make people uncomfortable because of how they work (physically uncomfortable) or what information they measure (socially uncomfortable)? Would you feel uncomfortable using such a system?

    ☐ Yes, because _____

    ☐ No

Participant Code: _____

35. If so, do you think you will be comfortable using it eventually?

    ☐ Yes

    ☐ No

36. Do you foresee any issues that may arise should such a system be used for authentication?

WRAP-UP SYSTEM 1

37. Overall, do you find **SYSTEM 1's** authentication method easy to use? If not, what problems have you experienced?

38. Would you consider the kind of authentication system employed in **SYSTEM 1** appropriate and acceptable for the task and environment?

39. If not, in your opinion, what kind of authentication system would work better?

OVERALL WRAP UP

40. Are there systems other than the four we've talked about, that have special characteristics, in terms of their passwords or authentication systems, that you'd like to talk about? For example, a system may have an unusual password system that you think is especially good or especially bad.

41. Is there anything else you'd like to tell us about authentication systems in general?