NISTIR 7991

United States Federal Employees' Password Management Behaviors – a Department of Commerce Case Study

Yee-Yin Choong
Mary Theofanos
Hung-Kung Liu

http://dx.doi.org/10.6028/NIST.IR.7991

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 7991

United States Federal Employees' Password Management Behaviors – a Department of Commerce Case Study

Yee-Yin Choong
Information Access Division
Information Technology Laboratory

Mary Theofanos
Office of Data and Informatics
Material Measurement Laboratory

Hung-Kung Liu
Statistical Engineering Division
Information Technology Laboratory

http://dx.doi.org/10.6028/NIST.IR.7991

March 2014

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

Table of Contents

List of Tables

List of Figures

1 INTRODUCTION

Passwords are still the most widely used authentication mechanism within the federal government. Alternatives exist such as the Personal Identity Verification (PIV) (2006) card mandated by Homeland Security Presidential Directive 12 (HSPD-12, 2004) which defines requirements for a standardized, United States (US) government-wide identification mechanism for gaining authorized access to federal facilities and federal information systems. The PIV card is universally used by federal employees for physical access, but the PIV card has still not universally replaced passwords for logical access. Even for those employees who use the PIV card for logical access, additional passwords are still required by many systems.

The literature describes many security and usability challenges with passwords. According to ISO standards [ISO 13407, 1999], usability is defined as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use." Adams and Sasse (1999) identified three usability characteristics that users want from passwords: passwords should be easy to remember, should be able to be used across multiple systems, and should rarely change. But this is in direct conflict with password security policies that require long passwords with high entropy, a unique password for each system, and passwords that users must change frequently. Florencio and Herley (2007) identified that the average web user has about 25 accounts that require passwords and a typical user types an average of 8 passwords per day. Zhang et al., 2009 identified that users must also attempt to remember the myriad of password policies for each of these accounts resulting in "access amnesia" and Adam et al., 1997 noted that this resulted in password interference.

Studies of password habits include surveys of organizational and individual behaviors of users. Password behaviors at work within organizations include studies by Adams and Sassse (1999). And, a large-scale observational study of password use and reuse by Florencio and Herley (2007) explored the password use and habits of individuals. A digest of recent surveys of password habits can be found at PasswordResearch.com[1] (http://www.passwordresearch.com). In general, these studies examine how users use and re-

[1] Specific products and/or technologies are identified solely to describe the experimental procedures accurately. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products and equipment identified are necessarily the best available for the purpose.

use passwords focusing on if users change passwords frequently, use complex passwords, and use short passwords. In addition, empirical studies have examined password selection, recall and memorability (Campbell et al., 2011; Haque et al., 2013; Vu et al., 2007; Yan et al. 2004; Zhang et al., 2009).

Few studies have focused on US federal government employees' password habits. Zviran and Haga (1999) investigated password characteristics such as length, composition, and password selection methods of the Department of Defense employees from a particular installation in California in 1999. At that time, there were no requirements on password length, complexity, and password change frequency. While these findings were groundbreaking at the time, government security policies and practices have changed significantly. Today within the federal government, password policies that enforce security practices with respect to minimum password length (anywhere from 12 to 16 characters or higher), complexity (alpha-numeric, upper and lower case and special symbols) and frequent change intervals are in place for all accounts. Since the federal government password policies predetermine these factors, we wanted to study users' password management behaviors, perceptions, attitudes and experiences with the policies in order to develop effective password policies that take into account security and usability considerations. Thus we developed a survey to collect data on users' password management behaviors with respect to their work accounts and not personal or social accounts.

The survey instrument was designed to explore the relationships between the length, complexity, and change interval of passwords and password management behaviors and security behaviors. For instance: are there possible associations amongst users' attitudes towards password policy requirements of length and complexity and users' password generation strategies or users' propensity to store and "write down" passwords or how frequently users experience login problems? Previous research reveals little about users' attitudes about the password policy requirements and password characteristics and behaviors.

2 METHODOLOGY

We designed an on-line survey to collect data on end-users' password management and their attitudes toward computer security in a government work environment. This paper focuses on the data collected from employees of the Bureaus of the US Department of Commerce (DOC) between June 2010 and June 2011. The survey was sent out via email to DOC employees asking for voluntary participation. They were informed that their responses would be collected anonymously to reduce possible social desirability bias and to encourage more honest responses (Ong and Weiss, 2000). To ensure anonymity, the chief information officer of each participating DOC bureau agreed that no personal identifiable information (such as IP address of the respondent's computer, email address, etc.) was collected or provided to us.

2.1 PROCEDURE

We selected the National Institute of Standards and Technology (NIST) to run a pilot of the survey. The pilot was rolled out one laboratory at a time. We sent out an email with a hyperlink to the survey asking for participation in a survey related to password management and usability. During the first laboratory rollout, it was brought to our attention that employees are very sensitive to inquiries related to passwords. The NIST security office received several reports from employees who thought they had received an email that was a phishing scam trying to elicit passwords. Employees were reluctant to click on the embedded link within the email. To resolve this issue, we shifted to a two-step approach: (1) laboratory management sent out an email informing employees about the research and to expect an email from the researchers; (2) we then sent out the email with the link asking for participation. No security reports were filed after the adoption of this two-step approach.

After the NIST pilot, the survey was conducted at nine other DOC bureaus. A similar two-step approach was utilized with a security officer from each participating bureau first sending out an email informing employees about an upcoming research survey on password management, and then a coordinator from each participating DOC bureau sending an email with a link to the research survey to its employees.

While completing the survey, the respondents were instructed to think about only work-related accounts that require authentications. The survey consists of nineteen questions related to password management and computer security and six demographic questions (see Appendix). These questions cover topics such as: number of work-related accounts requiring passwords, number of frequently[2] used passwords, number of occasionally used passwords, attitudes toward the bureau's password requirements (length, complexity, and change interval), password generation strategies, factors affecting password generation, time spent on generating passwords, password management, login problems, opinions on compromised passwords, and perception on cybersecurity training. On average, it took those who elected to take the survey about fifteen minutes to complete.

2.2 RESPONDENTS

At the time of the research, there were an estimated 38 000 DOC employees and a total of 4 573 (~ 12.0 %) DOC employees completed the survey. The major demographic characteristics of the respondents are listed in Table 1.

---

[2] We defined the phrase "frequently used password" as "used regularly at least once in a two-week span" since the US federal government has many systems running on a bi-weekly cycle, for example, time and attendance.

Table 1 Respondents' Demographic Characteristics

Characteristics	Category	%	Characteristics	Category	%
Age	<= 25	3.5 %	Federal Service	< 1	5.5 %
	26-35	20.5 %	Length (years)	1-3	15.1 %
	36-45	23.1 %		4-5	11.5 %
	46-55	29.8 %		6-10	7.7 %
	56-65	18.6 %		11-14	13.4 %
	>= 66	2.4 %		15 -20	11.3 %
	(not specified)	2.0 %		> 20	35.1 %
				(not specified)	0.5 %
Gender	Male	57.5 %	Job Levels	Executive	1.9 %
	Female	39.2 %		Manager	9.6 %
	(not specified)	3.3 %		Supervisor	13.8 %
				Team lead	11.5 %
				Non-supervisor	62.6 %
				(not specified)	0.6 %
Education	High school	7.0 %	Occupations	Physical science	25.7 %
	Associate	5.3 %		Information technology	14.3 %
	Bachelor	34.4 %		Biological science	9.5 %
	Master	31.7 %		Mathematics and Statistics	8.2 %
	Doctorate	15.6 %		General administration, clerical & office services	7.1 %
	Professional degree	2.7 %			
	(not specified)	3.3 %		Engineering & architecture	4.6 %
Computer Skill (self reported)	Novice	0.5 %		Accounting and budget	3.4 %
	Average	29.0 %		(Other)	27.2 %
	Advanced	50.6 %			
	Expert	19.5 %			
	(not specified)	0.3 %			

3 RESULTS

3.1 PASSWORD USAGE

On average, DOC employees had nine (range: 1 to 400) accounts at work that require logins. Due to the wide range of the data, medians were used for calculating the central tendency. The median of frequently used passwords was five (range: 0 to 105) and the median of occasionally used passwords was four (range: 0 to 245). Further breaking down the number of accounts requiring logins, showed that 21.8 % of the employees had less than or equal to five accounts, 41.5 % had between six to ten accounts, 25.4 % had between 11 to 20 accounts, and 11.0 % had more than 20 accounts.

3.2 ATTITUDES TOWARD PASSWORD POLICY AND REQUIREMENTS

In general, employees thought that their bureau has clearly communicated its password policy (very clear – 53.8 %, somewhat clear – 33.1 %). Although “using the same password for different accounts” is prohibited in most bureaus’ policies, the data showed otherwise (always – 17.9 %, more than half of my accounts – 19.8 %, about half of my accounts – 18.9 %).

Employees viewed the password requirements as burdensome: too long, too complex, and change too often. Over 70 % of the respondents preferred that a password stays valid for longer than 90 days before they have to change it. The responses are detailed in Table 2.

Table 2 Attitudes toward Password Requirements

Password Length	%	Password Complexity	%	Preferred Password Lifespan	%
Too long	56.9 %	Too complex	50.7 %	30 days or less	1.3 %
About right	36.0 %	About right	44.1 %	31-60 days	5.8 %
Too short	0.9 %	Too simple	0.6 %	61-90 days	18.7 %
No opinion/no response	6.2 %	No opinion/no response	4.6 %	91-120 days	18.2 %
				121-180 days	17.3 %
				181 days or more	35.0 %
				No opinion/no response	3.7 %

3.3 PASSWORD MANAGEMENT

3.3.1 Time spent on password generation

We asked respondents to estimate[3]: the average time spent on generating a password ($t_{freq.avg}$ for the frequently used passwords, and $t_{occ.avg}$ for the occasionally used passwords), and the longest time ever spent on generating a password ($t_{freq.max}$ and $t_{occ.max}$, respectively). If the number of frequently used passwords is n_{freq} and the number of occasionally used passwords is n_{occ}, we can estimate the total average time spent ($T_{freq.avg}$ and $T_{occ.avg}$) on generating passwords and the worst scenario ($T_{freq.max}$ and $T_{occ.max}$) when each password takes the longest time to generate, for each respondent (i), where

$$T_{freq,avg}(i) = t_{freq.avg}(i) * n_{freq}(i), \text{ and } T_{freq,max}(i) = t_{freq.max}(i) * n_{freq}(i)$$

$$T_{occ,avg}(i) = t_{occ.avg}(i) * n_{occ}(i), \text{ and } T_{occ,max}(i) = t_{occ.max}(i) * n_{occ}(i)$$

We can then find the means for $T_{freq,avg}$, $T_{freq,max}$, $T_{occ,avg}$, and $T_{occ,max}$, across all respondents. We can also calculate for the worst scenario how much time employees may spend on generating passwords annually based on a 90-day renewal cycle (i.e., four password changes a year), or a 60-day renewal cycle (i.e. six password changes a year). If every password takes the longest time to generate, an employee can spend from 12.4 hours (or 1.5 business days)

[3] The estimates ranged from few minutes to couple days. We had excluded estimates reported by respondents that were longer than two business days (i.e. 16 hours). Two business days were realistic scenarios since some systems will lock out users after unsuccessful password change attempts and incrementally lengthen the time between change attempts allowed.

at a 90-day cycle to 18.6 hours (or 2.25 business days) at a 60-day cycle each year generating passwords for their work. The results are in Table 3.

Table 3 Time Spent on Generating Passwords

Password type	Averages	Time Spent Annually (worst scenario)	
		Hours/employee/year (90-day cycle)	Hours/employee/year (60-day cycle)
Frequently used passwords	Mean ($T_{freq,avg}$) = 28.4 (min) Mean ($T_{freq,max}$) = 98.5 (min)	6.6 (h)	9.9 (h)
Occasionally used passwords	Mean ($T_{occ,avg}$) = 23.5 (min) Mean ($T_{occ,max}$) = 86.6 (min)	5.8 (h)	8.7 (h)
	Total	12.4 (h)	18.6 (h)

3.3.2 Considerations affecting password generation

Respondents answered the questions regarding the level of importance of each of the five factors (*Easy to enter/type*, *Easy to remember*, *Strong*, *Synchronized with passwords for other accounts*, and *Compliant with the password requirements*) that they considered when generating a password. The last factor *Compliant* was intentionally placed in the question to learn how important it is to respondents even though a password has to be compliant to be accepted by a system. These questions used a semantic-distance scale from "Not at all important" to "Very important." The percentage of respondents choosing "Very important" for each factor is in Table 4.

Table 4 Password Generation Considerations – rated "very important"

Considerations	Frequently used passwords	Occasionally used passwords
Easy to remember	81.0 %	63.8 %
Compliant with the password requirements	58.3 %	55.9 %
Synchronized with passwords for other accounts	45.8 %	36.8 %
Easy to enter/type	38.1 %	32.3 %
Strong	31.3 %	28.0 %

3.3.3 Password generation strategies

Respondents were given a list of password generation strategies and asked to check all that apply when generating their passwords. The results are in Figure 1.

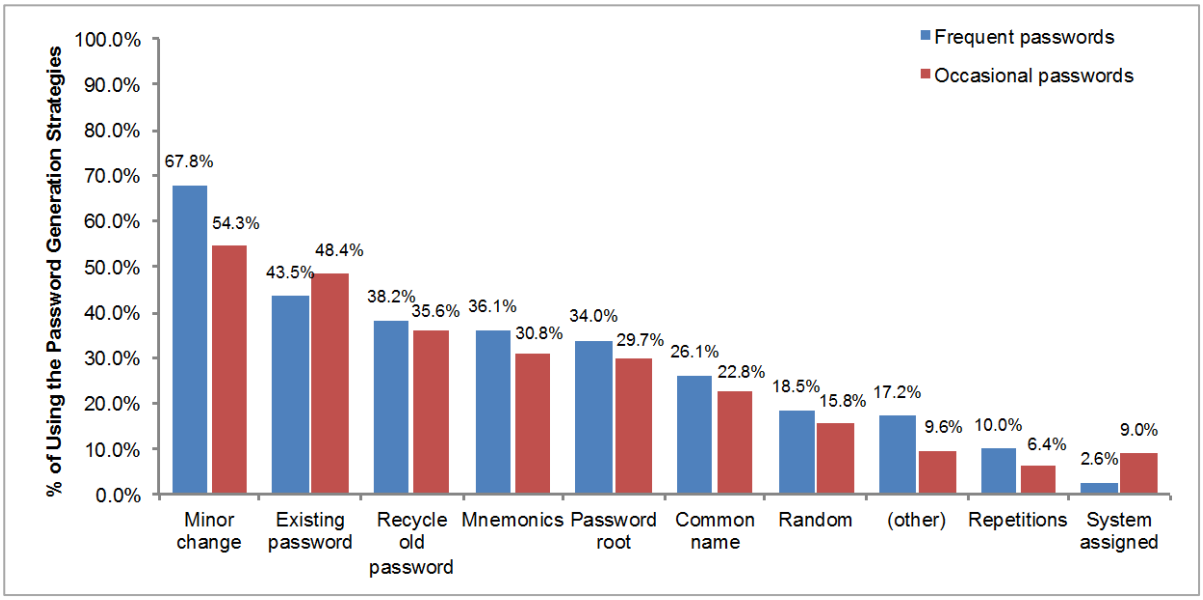

Figure 1 Strategies for generating passwords

3.3.4 *Password tracking methods*

Respondents were given a list of password tracking methods and asked to check all that apply. The results are in Figure 2.

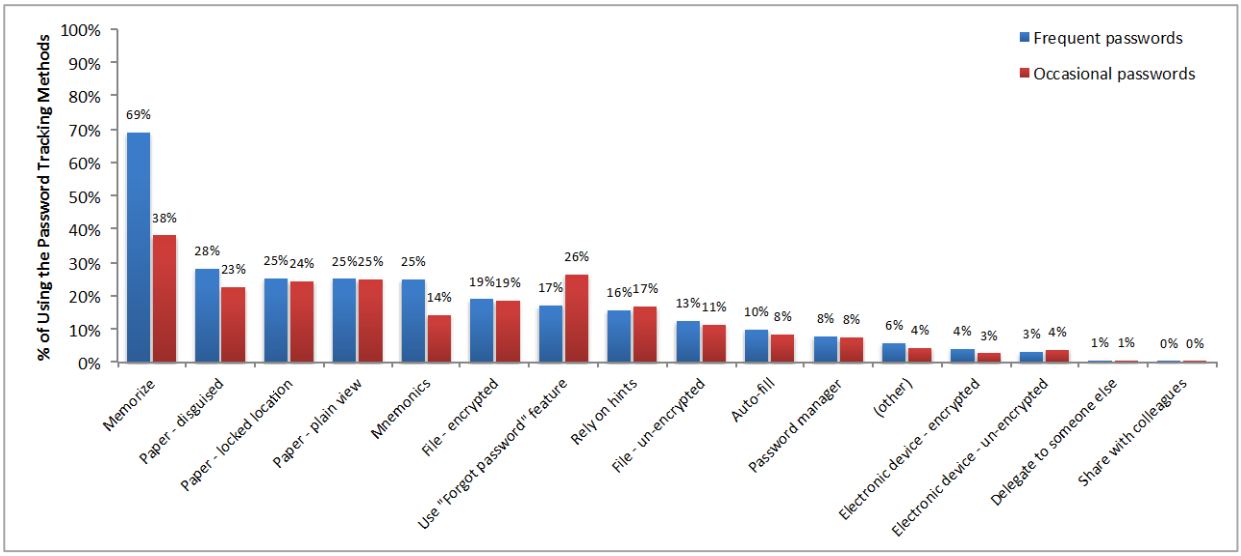

Figure 2 Password tracking methods

3.4 LOGIN PROBLEMS

Respondents were given a list of 11 common login problems and asked to indicate whether they had experienced such problems in the past six months and to rate the severity (*none*, *a little*, *some*, or *a lot*) in terms of perceived frustration level and time wasted. The top six login problems are listed in Table 5.

Table 5 Top Six Login Problems

Login Problems	Perceived Frustration Level			Perceived Time Wasted		
	A lot	*Some*	*(A lot + Some)*	*A lot*	*Some*	*(A lot + Some)*
Mistyping password	26.9 %	34.4 %	61.3 %	14.5 %	30.4 %	44.9 %
Forgetting password	24.1 %	39.9 %	64.0 %	16.8 %	37.5 %	54.3 %
Error message - password change	24.1 %	29.3 %	53.4 %	13.7 %	26.2 %	39.9 %
Multiple logins for single task	22.2 %	26.0 %	48.2 %	15.7 %	24.6 %	40.3 %
Forgetting which password to use	21.9 %	31.3 %	53.2 %	13.8 %	28.2 %	42.0 %
Getting locked out	19.0 %	28.8 %	47.8 %	18.1 %	26.7 %	44.8 %

3.5 ATTITUDES TOWARD OVERALL CYBERSECURITY AND USABILITY

We asked respondents to answer questions regarding their bureau's cybersecurity training: 93.5 % indicated that their bureau has offered training on cybersecurity, 4.1 % indicated "don't know" and 1.4 % indicated "no." Within those respondents who answered "yes," 58.8 % indicated that the training is useful (21.1 % - "very useful," and 38.7 % - "somewhat useful").

When asked about "how secure is the most frequently used password," respondents perceived their most frequently used password (most likely is their bureau-wide general password) as being *completely* (20.7 %) or *very* (43.9 %) secure.

There were two open-ended questions to solicit respondents' perceived consequences if their work-related passwords were compromised and to learn their views on what constitutes an ideal login process. Qualitative data analysis was performed on the free-text responses to those two questions.

3.6 PERCEIVED CONSEQUENCES FROM COMPROMISED PASSWORDS

Out of the 4 573 respondents, 3 927 provided responses to this question. Responses were analyzed and coded into concepts that were further organized into categories and sub-categories as listed in Table 6. Note that the percentages do not add up to 100 % as the percentages were calculated as the number of instances that a specific concept was mentioned in the responses divided by total number of 3 927 responses.

Table 6 Perceived Consequences from Compromised Passwords

Category	Sub-categories	%
Severity of consequences		
	Don't know/not sure	6.8 %
	None	22.8 %
	Minor	5.3 %
	Major	9.9 %
	Depending on accounts, by whom, and to what end	11.1 %
Data and Information		
	Personal info, Identity (PII) exposure/lost	14.9 %
	Data integrity (damaged/lost/modified)	10.8 %
	Sensitive government info at risk (e.g. espionage)	10.3 %
	Emails read/accessed	3.4 %
	Financial fraud/theft (e.g. Thrift Savings; credit card info)	2.8 %
	Time and attendance	0.5 %
	Travel manager (request, reimbursement, etc.)	0.5 %
Hacking		
	Gain unauthorized access to government systems/networks	7.9 %
	Security breach (infrastructure, functioning, security, resources, computer integrity)	6.5 %
	Misuse of account (e.g. send spam emails on behalf of me)	6.0 %
	Malicious software/malware	2.4 %
	Cyber attacks	0.7 %
	National security	0.3 %
Productivity		
	Disrupt business processes, lost productivity (e.g. recover lost data, time spent to reset accounts)	2.4 %
	Reset accounts (e.g. change all passwords)	1.6 %
	Account(s) locked out	1.3 %
	Loss of other passwords	0.2 %
Cost and Penalty		
	Employment reprimand (e.g. disciplinary action, dismissal)	4.2 %
	Security Reprimand/stricter policy/additional training	1.3 %
	Document compromises and investigation	0.6 %
	IT cost to organization (e.g. cleanup after break-in; disruption of systems/networks)	0.5 %
	Legal implications	0.2 %
Emotional Discomfort		
	Embarrassment to Organization	1.5 %
	Personal embarrassment	1.1 %
	Frustration, Inconvenience	0.8 %

3.7 IDEAL LOGIN PROCESS

There were 4 219 responses to this question. Concepts drawn from the responses covered a wide range of topics. Table 7 lists topics that had at least 150 (i.e., 3.5 %) occurrences in the free-text responses.

Table 7 Main Concepts for Ideal Login Process

Category	Sub-categories	%
Changes to current login process		
	Single signon	39.1 %
	Keep current process (same or similar)	4.1 %
Authentication factors		
What users are	Biometrics (modality unspecified)	8.4 %
	Fingerprint	15.6 %
	Iris	3.8 %
What users have	Smart card or badge	18.2 %
What users know	Username + password	4.7 %
	PIN	5.3 %
Policy and Requirements		
	Balance between user aspects (simple, quick and easy) and security aspects	4.1 %
	Reasonable and shorter password length	8.8 %
	Less frequent password change cycle	10.1 %

4 DISCUSSION

4.1 PASSWORD INTERFERENCE

From the results, we learn that US employees have about nine passwords that they need to manage at work. While the average user has nine accounts, alarmingly there is about 25 % of the DOC employees have between 11 and 20 accounts that they need to manage at work. We find that respondents spend quite a lot of time just generating passwords when old ones expire. We realize that the time to manage those passwords can grow significantly when we start thinking about the entire user password management lifecycle: generation, maintenance/tracking, and authentication (i.e. entering/typing the passwords numerous times throughout each work day). Besides time, there is also an economic or productivity impact as employees have to shift away from their main tasks (Monsell , 2003; Czerwinski, et al. 2004) to attend to the activities required to manage their passwords such as generating and keeping track of their passwords and logging into accounts/systems constantly. Steves et al. (2013) reported from their diary study that, on average, a user performed logins 23 times in a typical workday. These password management activities are disruptive to their work and can impact employees' productivity.

Although the bureaus have done a good job on communicating their password policies to their employees, these policies undermine employee productivity and result in behaviors that actually lower security. The password requirements have become more and more stringent (long passwords, complex composition rules, and frequent change cycles) over the past decade and have imposed a huge burden on the end-users. Many respondents have expressed their frustration toward the requirements. One stated, "I understand that for 'security' reasons it is good to change a password - but seriously are we all expected to magically remember 12 different passwords, most of which are 10 charecters[sic] long, and can't look like a word (I

agree with the reason for the complexity - it just hard on the user).*"* Another respondent said, "Security has become so complex, it's interfering with being able to do a job efficiently.*"*

4.2 TOP CONSIDERATION – *EASY TO REMEMBER*

When generating passwords, *Easy to remember* is the most important consideration: 81.0 % for frequently used passwords and 63.8 % for occasionally used passwords. *Compliant* comes as the second most important consideration with 58.3 % and 55.9 % for frequently used passwords and occasionally used passwords, respectively. One would expect a higher percentage for *Compliant* as the systems would reject any non-compliant passwords. However, there are only a little over 50 % of the respondents who view *Compliant* as very important during the password generation process. As one respondent put it, "Compliance requirement is very important only because it's required." Interestingly, *Strong* is the least important factor that only 31.3 % choose "Very important" for the frequently used passwords and 28.0 % for the occasionally used passwords. One respondent explained the phenomena perfectly, "The password requirements make the password hard enough for me to remember that I am not worrying about if someone can crack it as much as if I will be able to use it."

Minor change, *existing password*, and *recycle old password* are the top three strategies used by the employees. It is apparent that employees are trying to minimize the need to memorize new information that adds to their already cluttered memory of multiple passwords.

4.3 PASSWORDS "WRITTEN DOWN" BESIDE MEMORIZATION

When people have more information than they can hold in their memory, it is impractical and unreasonable to forbid the use of tools to keep track of the information. As we learn from the results, many respondents (69.0 %) use *memorize* to keep track of their frequently used passwords, but many fewer (38.2 %) can do so with their occasionally used passwords. Respondents have to use other mechanisms to manage their passwords, such as writing them on paper, saving them in a file, password managers, or electronic devices. We recoded the data to two new variables: (1) *paper (at least one)* which counts the occurrences of respondents checking at least one among *paper-disguised*, *paper – locked location*, and *paper – plain view*; and (2) *storing* which counts the occurrences of respondents checking at least one from any of the storing methods: paper, file, electronic device, or password manager. The comparison of three primary tracking methods is shown in Figure 3. Over 80 % of the respondents use at least one *storing* method (paper, file, electronic device, or password manager) to track their frequently and occasionally used passwords. While 69 % of the respondents use *memorize* to track their frequently used passwords, the percentage dropped significantly (38 %) when it comes to tracking their occasionally used passwords.

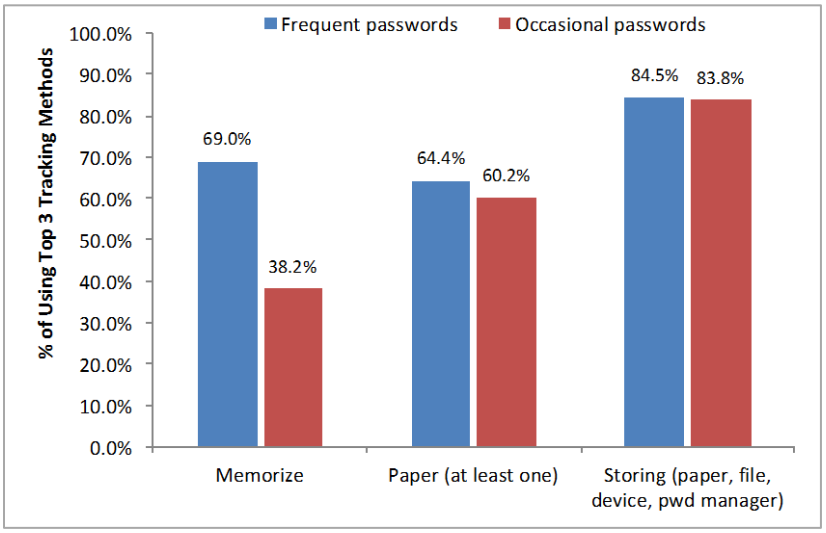

Figure 3 Comparison of primary tracking methods

4.4 MORE PASSWORDS MEANS MORE LOGIN PROBLEMS

Not surprisingly, the top two login problems causing frustration are mistyping passwords and forgetting passwords. Getting locked out is perceived as the biggest waste of time.

Furthermore, we investigate the relationship between the number of passwords (frequent and occasional) and the severity of a login problem (frustration level and time wasted) for all eleven login problems listed in the survey. The survey was designed with naturally ordered response categories for severity (none, a little, some or a lot) for both the frustration level and the amount of time wasted from each login problem. We observe a clear pattern between the number of passwords a user has and the severity of login problem he/she perceives—as the number of passwords increases, severity increases as well. To quantify the significance of this relationship, we considered the number of passwords as a function of the severity of a login problem. We tested the null hypothesis of homogeneity: the number of passwords has no effect on the severity of the login problems against order restricted alternatives: the more passwords the more severe the problems. In particular we calculated the likelihood ratio test that has been shown (Barlow et al., 1972; Robertson et al., 1988) to be proportional to the residual sum of squares from fitting the monotonic (isotonic) regression of the observed number of passwords with respect to the natural order of severity levels. We have done this minimization numerically using the function `isoreg` from the R environment for statistical computing and graphics (R Development Core Team, 2012).

To estimate the sampling distribution of the likelihood ratio test statistic, we need many samples generated under the null hypothesis. By randomly shuffling the number of passwords, we can simulate the survey results many times. If the null hypothesis is true, the

shuffled data sets should look like the real data. The ranking of the real actual test statistic among the shuffled test statistics gives the *p*-value. Our results confirm that the more passwords (frequent and occasional) an employee has, the more he/she experiences frustration and time wasted from login problems. It is statistically significant ($p < 0.01$) across all eleven problems listed in the survey.

Employees are overwhelmed by stringent password requirements, multiple passwords, and frustrated by the login problems such as mistyping passwords and forgetting passwords. They want to reduce the burden of having to manage multiple passwords and call for improvement to current login process. Almost 40 % of the respondents mention single sign-on to be their ideal login process. Many mention the willingness to accept longer and more complex password that does not change often as one respondent put it, "A complex password which is very difficult to hack and can be kept indefinitely unless you think it has been compromised. One that can be used for all systems."

4.5 SECURITY AS EXTERNALITY

An alarming finding is that employees seem to have a false perception of security around their work-related accounts. The respondents view their most frequently used password as highly secure. They think that their bureaus are responsible for their bureau's cybersecurity and thus, more than 1/3 of the respondents (~35 %) perceive no major consequences (or risk to their agency) if their passwords were compromised. Some stated, "very little; computers behind regional firewall; accounts have limited privileges," and "My work is for public consumption."

Very few respondents mention more serious security consequences that could result from passwords being compromised, e.g., gaining access to other systems, security breach, spamming, malware, or cyber attacks. The instances of those concepts are all below 10 %. Employees focus more on the impacts to their individual work rather than the bigger picture of their agency.

4.6 IMPORTANCE OF EMPLOYEES' ATTITUDES TOWARD PASSWORD REQUIREMENTS

While the majority of the respondents view the length and complexity requirements as *burdensome* (i.e. too long, too complex), there are still a good number of respondents who are quite receptive to those requirements (36 % selected *about right* for password length and 44 % selected *about right* for password complexity). This leads us to investigate whether these dichotomous views hold any relationships to employees' password management behaviors.

4.6.1 Password generation considerations vs. attitudes toward password requirements

We plot the data from the top two considerations, *Easy to remember*, *Compliant*, and the least concerned consideration *Strong* against the dichotomous views toward the length and complexity requirements (Figure 4). It shows that *Easy to remember* is more important for respondents who find the requirements burdensome compared to those who find the requirements *about right*. Interestingly, it is the opposite for *Compliant* and *Strong*. The difference between the *burdensome* respondents and the *about right* respondents is about 15 % for *Compliant*, whereas for *Strong*, the percentage of the *burdensome* respondents is almost half of the percentage of the *about right* respondents.

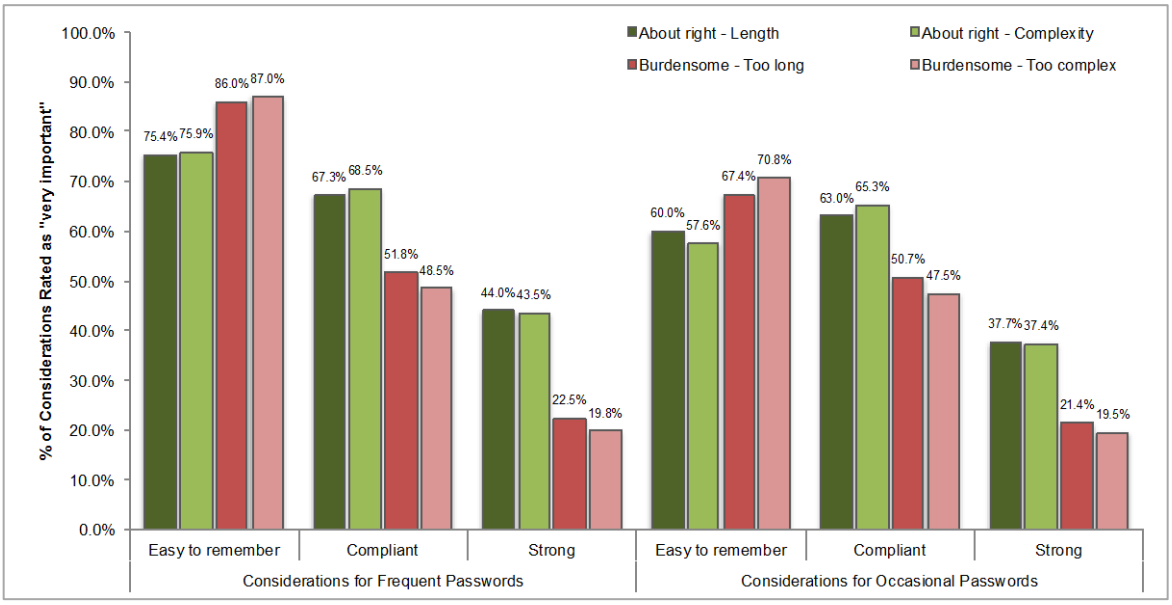

Figure 4 Password generation considerations vs. attitudes toward requirements

4.6.2 Password generation strategies vs. attitudes toward password requirements

We examine the relationships among the top three password generation strategies and employees' attitudes toward the length and complexity requirements. Figure 5 shows that respondents tend to use the strategies of *Minor change*, *Existing password*, and *Recycle old passwords* more when they view the length and complexity requirements as *burdensome* compared to those who think the requirements are *about right*. The differences range from 7 % to 12 %.

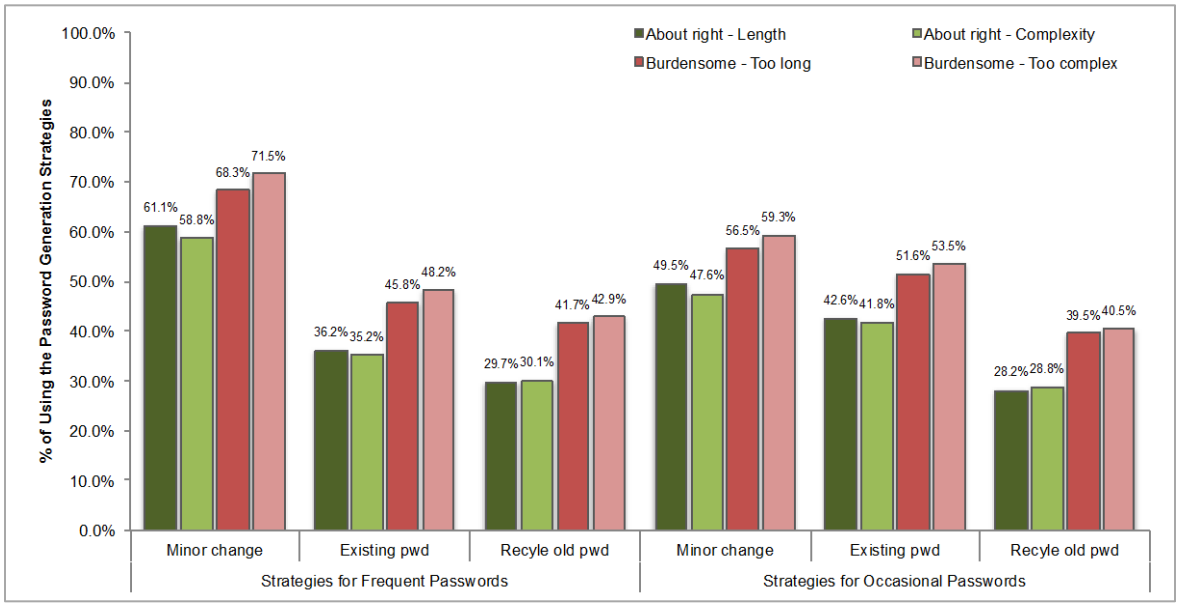

Figure 5 Top 3 password generation strategies vs. attitudes toward requirements

4.6.3 Storing, or "Write down," passwords vs. attitudes toward password requirements

Generally, when respondents think the passwords requirements are *burdensome*, they use memorization less, record on paper more, and store in files more, compared to respondents who think the requirements are *about right* (Figure 6).

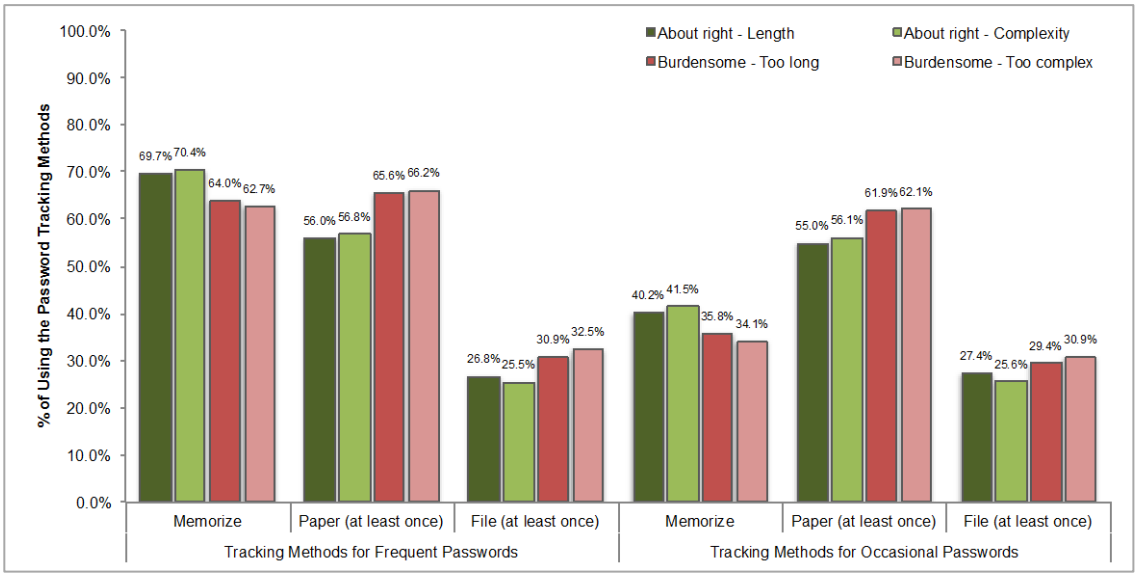

Figure 6 Primary Tracking Methods vs. Attitude toward Password Requirements

This phenomenon is even more prominent when we examine the data further by looking at only the method of writing passwords on paper in plain view, for example, on a sticky note next to a computer. In Figure 7, it shows that there is about a 50 % drop of writing on paper in plain view when respondents think the requirements are *about right*, compared to *burdensome* respondents. When we further narrow it down to respondents who chose both *about right* and respondents who chose both *too long* and *too complex* on the requirements, the drop is more than 50 %.

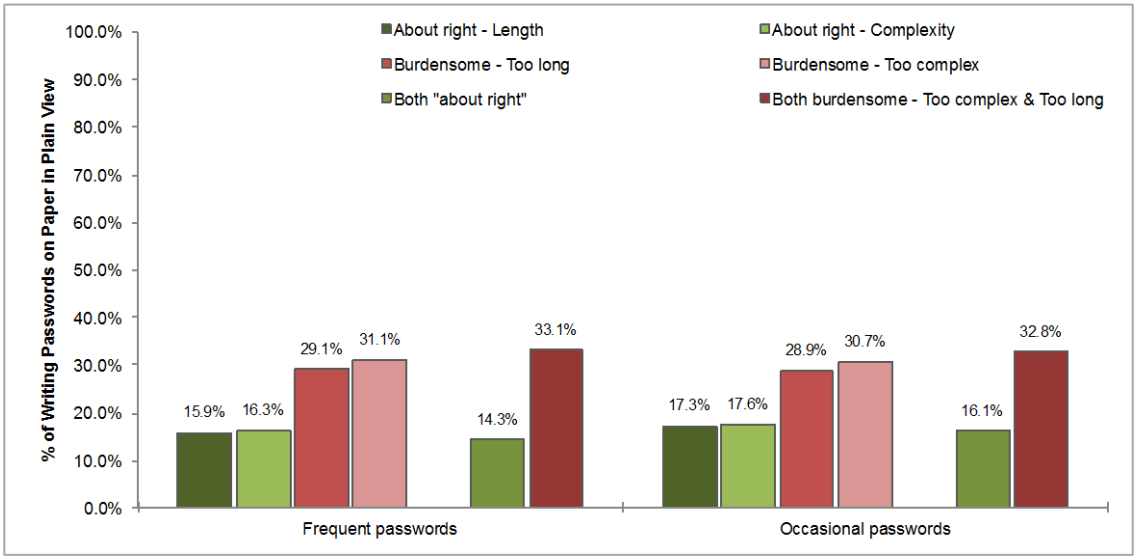

Figure 7 Passwords on paper in plain view vs. attitudes toward requirements

4.6.4 Login problems experience vs. attitudes toward password requirements

When respondents view the requirements as *about right*, they are less likely to perceive *a lot* of frustration experienced with the login problems. Figure 8 shows this relationship for the top three login problems: mistyping password, forgetting password, and getting error messages while changing a password. A significant finding is that the *burdensome* respondents perceive about twice as much frustration with those login problems compared to the *about right* respondents.

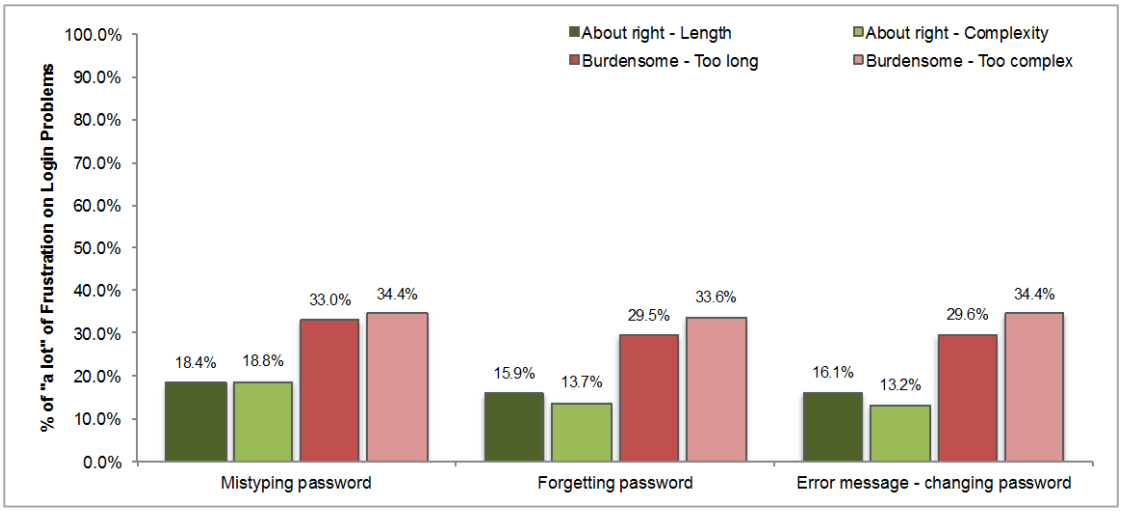

Figure 8 Frustration with top 3 login problems vs. attitudes toward requirements

4.6.5 Perception on compromised passwords vs. attitudes toward password requirements

As listed in Table 6 on perceived consequences from compromised passwords, majority of the responses are related to the severity of consequences (total occurrences of 55.9 %). We are surprised that a large number (35 %: 6.8 % – *Don't know*, 22.8 % – *None*, and 5.3 % – *Minor*) of the responses do not perceive major consequences (9.9 % mentioned *Major* consequences) from potential compromises of the work-related passwords. Further examining the data, we make an important discovery on the relationship between the perceived severity of consequences from compromised passwords and the employees' attitudes toward the password requirements (Figure 9). While the perception of "minor" consequences and "don't know" are about the same across different groups, it is clear that the *about right* respondents are much less likely to answer "no consequences" (-14 % for length requirement, and -17.4 % for complexity requirement) and they are more likely to perceive "major consequences" (+7.1 % for length, and +7.8 % for complexity) when their work-related passwords are compromised. Another interesting finding is that the *about right* respondents are more likely to gauge the consequences depending on the types of accounts that the passwords might be compromised (+6.7 % for length, and +6.6% for complexity). If we restrict the data further to look at the group of choosing both *about right* for the length and complexity requirements and the group of stating both as too *burdensome*, i.e. "too long" and "too complex," we find the same trends with bigger differences. For example, the both *about right* group is 21.3 % less likely to perceive "no consequences," 10.5 % more likely to perceive "major consequences," and 8.1 % more likely to gauge consequences depending on accounts.

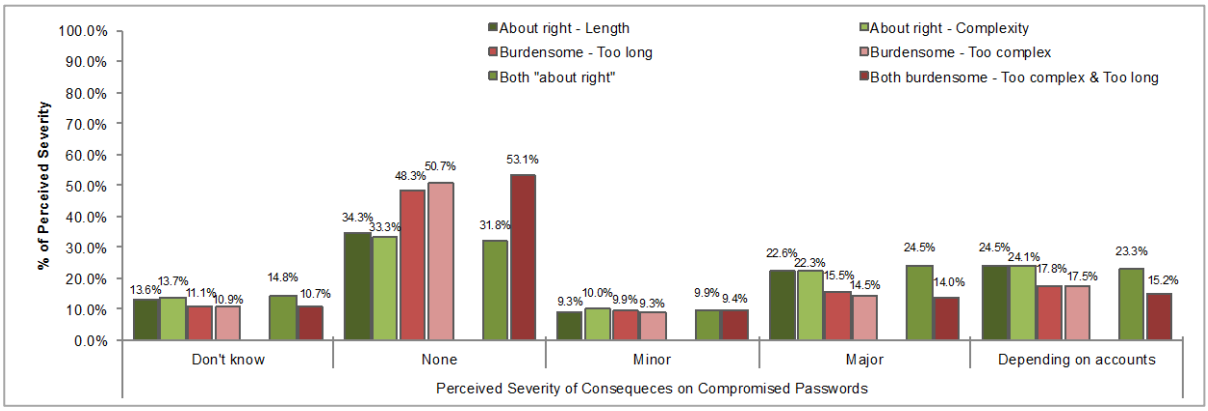

Figure 9 Perceived severity of consequences vs. attitudes toward requirements

5 CONCLUSIONS

The combination of the current password policies and the number of accounts requiring passwords has pushed the limits of human cognition. The federal employees in this survey have been overwhelmed by the user password management lifecycle consisting of three stages: password generation, password maintenance, and authentication itself. As a result, in order to perform their jobs effectively, they have to employ coping mechanisms such as choosing *easy to remember* passwords and "*write down*" *storing* of their passwords.

A key finding of this study is that employees' attitudes toward the rationale behind cybersecurity policies affect their behaviors and experiences. The results indicate that positive attitudes about password requirements such as complexity and length correlate with more secure behaviors and positive experiences:

- Good password management behaviors such as choosing stronger passwords
- "*Write down*" passwords less often, more likely to memorize passwords
- Less frustration with login procedures
- Better understanding and respecting the significance of the need to protect passwords and system security.

The converse is also true that negative attitudes correlate with:

- Poor password management behaviors such as not caring about password strength
- "*Write down*" passwords more often, less likely to memorize passwords
- More frustration with login procedures
- Not understanding and caring about the significance and the need to protect passwords and system security.

About 40 % of the respondents requested single sign-on as a better login process to alleviate the complexity of the password policies. A possible solution is to implement logical access to all accounts using the PIV card. A follow-up survey of employees who use the PIV card for logical access in other federal agencies should provide insight into the effectiveness of this solution.

We need more research to investigate factors on promoting positive attitudes toward cybersecurity in general and passwords in particular. We need to understand users' cognitive processes during the three stages of the password management lifecycle. Finally, organization policies may need to be updated and training may need to be re-examined for its effectiveness.

6 REFERENCES

[1] Adams, A., Sasse, M. A., & Lunt, P. (1997). "Making Passwords Secure and Usable." *People and Computers XII*: 1-19.

[2] Adams, A., & Sasse, M. A. (1999). "Users are not the enemy." *Communications of the ACM* **42**(12): 40-46.

[3] Barlow, R. E., Bartholomew, D. J., Bremner, J. M., & Brunk, H. D. (1972). *Statistical inference under order restrictions*. London: Wiley.

[4] Campbell, J., Ma, W., & Kleeman, D. (2011). "Impact of restrictive composition policy on user password choices." *Behaviour & Information Technology*, 30(3), 379 - 388.

[5] Czerwinski, M., Horvitz, E., & Qilhite, S. (2004). "*A diary study of task switching and interruptions" Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 175-182).

[6] Florêncio, D., & Herley, C. (2007). "A Large-Scale Study of Web Password Habits." *Proceedings of the 16th international conference on World Wide Web 2007*, 657 - 666.

[7] Haque, S. M. T., Wright, M., & Scielzo, S. (2013). "A Study of User Password Strategy for Multiple Accounts*." Proceedings of the Conference on Data and Application Security and Privacy 2013*, 173 - 175.

[8] HSPD-12 (2004, August 27). Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors.

Retrieved September 23, 2013, from http://www.dhs.gov/homeland-security-presidential-directive-12#1

[9] International Organization for Standards. ISO 13407 Human-centered design process for interactive systems, Geneva, Switzerland, (1999).

[10] Monsell, S. (2003). Task switching. *Trends in Cognitive Sciences, 7*(3), 134-140.

[11] National Institute of Standards and Technology. (2006). *Personal identity verification (PIV) for Federal employees and contractors.* FIPS PUB 201-1 (2006).

[12] Ong, A. D., & Weiss, D. J. (2000). "The Impact of Anonymity on Responses to Sensitive Questions." *Journal of Applied Social Psychology*, 30(8), 1691-1708.

[13] R Development Core Team. (2012). *R: A Language and Environment for Statistical Computing.* R Foundation for Statistical Computing, Vienna, Austria, ISBN 3-900051-07-0. URL http://www.R-project.org

[14] Robertson, T., Wright, F. T., & Dykstra, R. L. (1988). *Order Restricted Statistical Inference*. New York: Wiley.

[15] Steves, M., Chisnell, D., Sasse, A., Krol, K., Theofanos, M., & Wald, H. (2013). *Authentication Diary Study*. NISTIR, National Institute of Standards and Technology, Gaithersburg, US.

[16] Vu, K.L., Proctor, R.W., Bhargav-Spantzel, A., Tai, B., Cook, J., & Schultz, E. E. (2007). "Improving password security and memorability to protect personal and organizational information." *International Journal of Human-Computer Studies*, 65, 744-757.

[17] Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). " Password Memorability and Security: Empirical Results." *IEEE Security and Privacy* Sept/Oct, 25-31.

[18] Zhang, J., Luo, X., Akkaladevi, S., & Ziegelmayer, J. (2009). "Improving multiple-password recall: an empirical study." *European Journal of Information Systems*,18(2), 165 - 176.

[19] Zviran, M., & Haga, W. J. (1999). "Password Security: An Empirical Study." *Journal of Management Information Systems*, 15(4), 161 - 184.

APPENDIX A: QUESTIONS IN THE FEDERAL EMPLOYEE PASSWORD USABILITY SURVEY

Questions about all work-related accounts that require logins

1. How many work-related accounts do you have that require a password?
   (e.g., for computers, network, email, time and attendance, travel, training, etc.)

2. How often do you use the same password for different accounts at work?
   - Never or almost never
   - Less than half of the time
   - About half of the time
   - More than half of the time
   - Always or almost always

3. How clearly does your agency communicate the details of its password policy to you?
   (e.g., must fulfill password creation requirements, password expiration, password must be protected, etc.)

   - Not at all clearly
   - A little clearly
   - Somewhat clearly
   - Very clearly

4. What do you think of your agency's password requirements?
   (e.g., password length, use of special characters, password lifespan, etc.)

   4a. Password length - minimum number of characters required

   - Too short
   - About right
   - Too long
   - Don't know/No opinion

   4b. Complexity of the password requirements

   - Too complex
   - About right
   - Too simple
   - Don't know/No opinion

   4c. In your opinion, how many days should a password remain valid before you have to change it?

- 30 days or less
- 31 - 60 days
- 61 - 90 days
- 91 - 120 days
- 121 - 180 days

5. How many work-related passwords do you use frequently?
   (i.e., used regularly at least once in a two-week span)

6. What strategies do you use to create frequently used passwords for work? (check all that apply)
   - Create from a password root (e.g., 2PwdRt&, PwdRt42%, or tXpwdRT@)
   - Let system assign password
   - Make minor change(s) to an existing password (e.g., %elvis1, #elvis2, or $elvis3)
   - Recycle old passwords (e.g., old passwords that are not in current password history)
   - Use a common name, word, or phrase (e.g., Boston12)
   - Use a meaningful mnemonic (e.g., 2beOrnOt@toBee from "to be or not to be")
   - Use a random combination of words, letters, or characters
   - Use character repetitions (e.g., !!!AAAbbb999)
   - Use existing passwords from other accounts
   - Other –describe strategies generically and do not provide an example of an actual password or enough information to infer your password

7. Please rate how important the following considerations are to you, when you create a frequently used password for work.

	Not at all Important	Only a little Important	Somewhat Important	Very Important
Easy to enter/type				
Easy to remember				
Strong, i.e., hard to guess/crack				
Synchronized with passwords for other accounts				
Compliant with the password requirements				

8. Please estimate the time it takes you to create a frequently used password for work.
   (Please include the time that you spend to consider all factors, e.g., comply with password requirements, use the same from other accounts, etc.)

   Average Time: _____ (e.g., 30 seconds, 5 minutes, etc.)

   Longest Time: _____ (e.g., 45 minutes, 2 hours, etc.)

9. How do you keep track of your frequently used passwords for work? (check all that apply)

- Do not track, use “forgot password” feature
- Have someone (e.g., secretary) manage passwords for you
- Let browser auto-fill
- Memorize the passwords
- Rely on hints provided by system
- Save in a document/file, protected with encryption or password
- Save in a document/file, not protected (i.e., without encryption or password)
- Share with a colleague, in case you forget
- Store in unencrypted electronic devices, e.g., USB key, PDA, cell phone, etc.
- Store in agency-managed, encrypted electronic devices, e.g., BlackBerry
- Use mnemonics, e.g., meaningful phrase
- Use password management software
- Write down on paper, but disguise in some way (e.g., only write down the common word without the special characters)
- Write entire password down on paper and store securely in a locked location
- Write entire password down on paper and place in a non-locked location
- Other – please describe

10. In your opinion, how secure is your most frequently used password at work?
    - Not at all secure, i.e., very easy to guess/crack
    - Slightly secure
    - Moderately secure
    - Very secure
    - Completely secure, i.e., extremely hard to guess/crack
    - Don’t know

11. – 15. (repeat questions 5-9 for occasionally used passwords.)

16. In the past 6 months, how much frustration and time have these problems caused you?
    16a. Frustration with problems

	None	A little	Some	A lot
Forgetting your User name or ID				
Forgetting your password				
Forgetting your PIN				
Forgetting which password goes with which account				
Getting locked out of an account				
Mistyping a password				
Getting error messages when trying to change a password				
Getting error messages when trying to recover a password				
Dealing with slow or unhelpful system support				
Valid password rejected for unclear reason				

Single task requiring different logins to multiple applications, i.e., task flow interrupted by multiple logins				

16b. Time wasted on problems

	None	A little	Some	A lot
Forgetting your User name or ID				
Forgetting your password				
Forgetting your PIN				
Forgetting which password goes with which account				
Getting locked out of an account				
Mistyping a password				
Getting error messages when trying to change a password				
Getting error messages when trying to recover a password				
Dealing with slow or unhelpful system support				
Valid password rejected for unclear reason				
Single task requiring different logins to multiple applications, i.e., task flow interrupted by multiple logins				

17. What consequences, do you think, would there be if your passwords were compromised?

18. Does your agency provide training on cyber security?
    - Yes
    - No
    - Don't know

    18a. If yes, how useful is your agency's training on cyber security?

    - Not at all useful
    - A little useful
    - Somewhat useful
    - Very useful

19. What would be the ideal login process for you?

Basic Demographic Information

1. Please answer the following questions about your job in the federal government.
   1a. What is your supervisory status?

    - Non-supervisor
    - Team leader
    - Supervisor
    - Manager
    - Executive

1b. Which occupational group does your job fall under?

2. How long have you been working in the Federal Government?
   - Less than 1 year
   - 1 to 3 years
   - 4 to 5 years
   - 6 to 10 years
   - 11 to 14 years
   - 15 to 20 years
   - More than 20 years

3. Gender
   - Male
   - Female

4. What is your age group?
   - 25 and under
   - 26-35
   - 36-45
   - 46-55
   - 56-65
   - 66 and above

5. What is your highest education (degree/level attained)?
   - High school or equivalent
   - Associate degree
   - Bachelor's degree
   - Master's degree (e.g., MS, MA, etc.)
   - Doctoral degree (e.g., PhD)
   - Professional degree (e.g., MD, JD, etc.)
   - (other)

6. How would you rate your level of experience using computers?
   - Novice
   - Average
   - Advanced
     Expert