ENHANCING SECURITY FOR PUBLIC EMPLOYEES

CSPRA
COALITION FOR SENSIBLE PUBLIC RECORDS ACCESS

Executive Summary

The purpose of this short paper is to inform policy makers of possible ways to address growing threats against public employees. We make the following recommendations and findings:

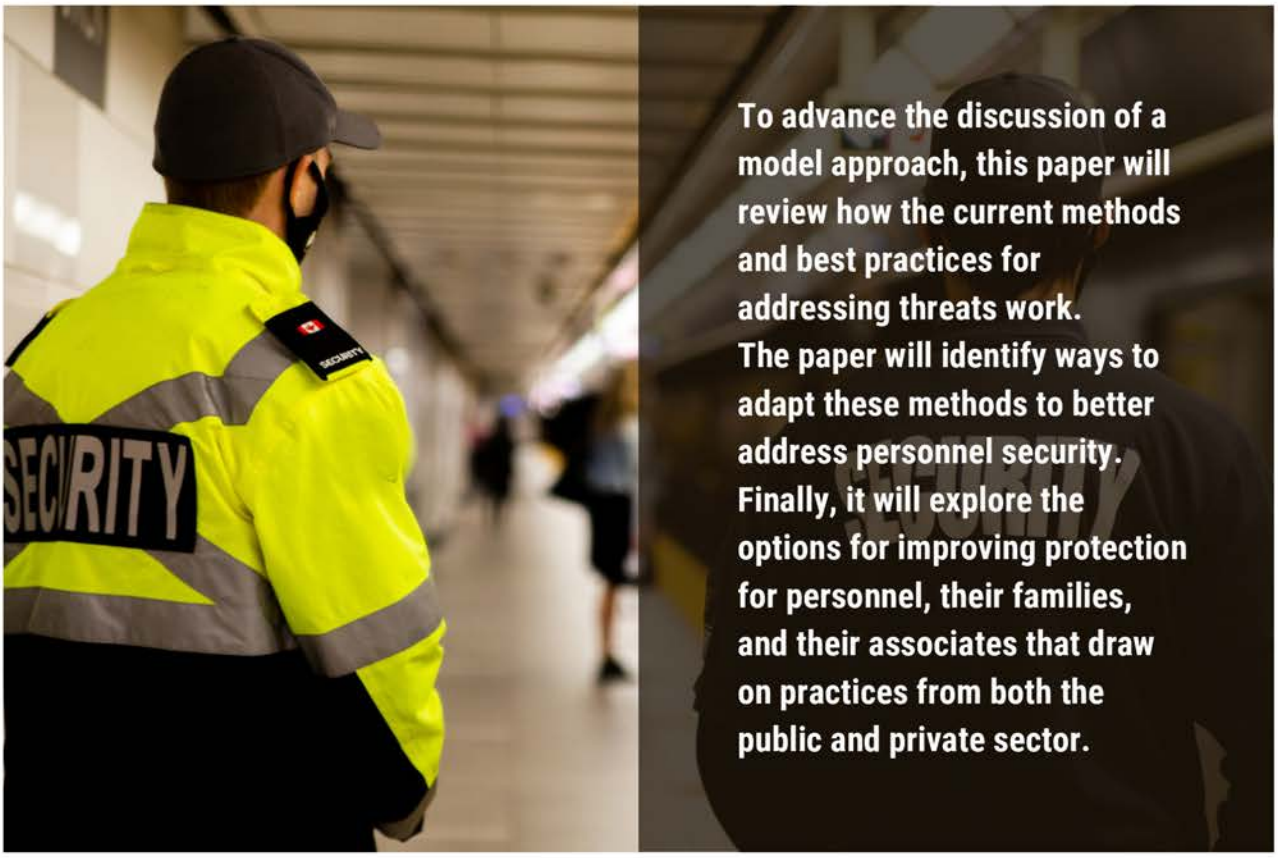
- Threats against public employees are growing and merit a comprehensive and effective response.
- We must take this threat seriously and match the threats with processes, programs, and laws that will reduce and prevent risks, deter bad actors, and apprehend and punish those who break the law while targeting public employees.
- Redaction of employee address is an ineffective response and amounts to security theater while doing real harm to the many beneficial uses of public records for public oversight and everyday transactions.
- Existing all-threat management techniques provide an excellent methodology to identify threats and countermeasures worth pursuing.
- Current threat assessments have not fully accounted for new threats and threat targets (e.g., extended family members and staff) and venues (such as homes and other locations away from the traditional workplace).
- There are existing laws and models that can provide excellent insights into how to address these threats.
- Current federal and state laws need to be reviewed and better applied to this risk and new laws may be needed to address the new and emerging issues.
- We lack any solid evidence that informational obscurity on addresses will deter the determined who have the capacity for violence and harmful behavior.
- The times demand and public employees deserve a more complete set of policies and programs to enhance public employee safety that goes beyond the single, weak, and ineffective concept of address redaction to a more 'security-in-depth' approach.

INTRODUCTION

Note: *This is a continuing work in progress. It is intended to facilitate discussion about how best to enhance security of public employees.*

The purpose of this short paper is to inform policy makers of possible ways to address growing threats against public employees. The US Federal, State, and Local Governments have responded to threats and incidents in recent years by adopting robust threat analysis/planning/response laws, rules, plans, budgets, training, programs, governance, and operational entities. These efforts fall into two main categories. The first is infrastructure including government buildings as well as public and private physical assets like transportation assets, power grids, water treatment plants, and dams. The second is digital assets and cybersecurity. While both categories address personnel security to some extent, neither of them focusses on protecting employees and officials nor do they fully reflect the current threats that go beyond the physical workplace and government computer systems. The problem is that most of the effort has gone into protecting the buildings. It was assumed that was the primary way to protect the people who work in them. However, this should now be seen as insufficient given the current environment and threat matrix.

The existing security regimens for physical and cyber security have the right methodologies to address the broader threats to personnel. What is needed is a model approach to making sure threats to personnel are properly included in threat management and risk reduction and that the range of methods and countermeasures is expanded and deployed to address the wider range of current and emerging threats.



BRIEF THREAT MANAGEMENT OVERVIEW

The threat categories of interest here are crime (physical and cyber), civil disturbance, reputational harm, and tortious harm to persons and property. The threat targets of concern for the purposes of this paper are people, buildings/facilities where government employees work and live, and goodwill/public trust.

The key elements to threat management methods include the following: survey of threats, assessment of threats, determination of countermeasures, decisions on risks to accept and those to address with available or new resources, and evaluation of maturity, quality, and efficacy of the methods and outcomes. What follows is a more detailed description of these key elements and others that build and maintain a complete security plan.

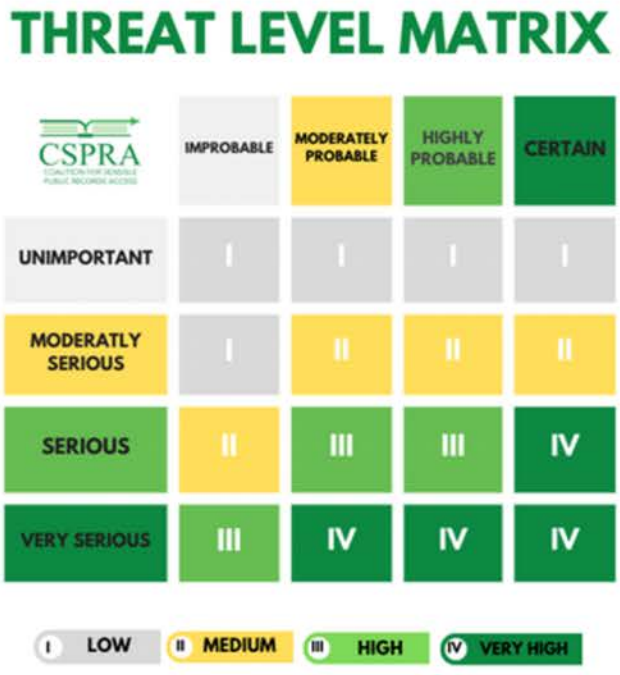
Survey of Threats

An all-threats approach begins with a wide view of the possible threats. The threats can be singular and combinatory (combining a cyber-attack with a physical one for example) and should be part of an overall risk assessment process for an entity. In other words, do not survey threats in isolation but in the context of the jurisdiction and its overall risks as this allows for better alignment and prioritization of responses later.

The threats and threat targets are typically listed within categories. Several of these threat categories and threat targets are beyond the scope of this analysis such as the threat category of natural disasters and the threat target of public utilities. The threat categories of interest here are crime (physical and cyber), civil disturbance, reputational harm, and tortious harm to persons and property. The threat targets of concern for the purposes of this paper are people, buildings/facilities where government employees work and live, and goodwill/public trust.

Assessment and Prioritization of Threats

Risk managers have time-tested methods of enumerating and prioritizing threats. These methods have been honed and committed to rote practice since the terrorist attacks on 9/11 and various other events that have disrupted our lives. The methods can be easily applied in this context to create a complete description of the threat categories and targets listed above and any others considered emergent or relevant. These descriptions identify the frequency, trends, threat vectors, sources, targets, and types of attacks and acts that can be part of the threat. These are then used to create a threat level matrix, like the kind shown above, which in turn is used to determine which threats to address and what methods and countermeasures are warranted for a given threat.



Selection of Methods and Countermeasures to Reduce Risk

Once the threats and targets are identified and ranked based on degree of probability and level of importance, then the available and needed methods and countermeasures for addressing those threats against those targets are inventoried, cost-benefit analyzed, and chosen based on a variety of factors that focus on optimizing risk reduction. The chosen methods and countermeasures will be assigned a cost, a cost avoidance, and a return on investment that weighs the costs against the reductions in risk to find the best ways to use the (always) limited resources available to accomplish the goal of making public service empoloyment safer.

Alignment of Resources and Costs with Desired Level of Risk Reduction

After the methods and countermeasures are identified, the risk tolerance level of the leadership that allocates resources is determined, the level of resources needed to reach that level of acceptable risk is calculated, and the available resources are compared to what is needed. If resources are available, adequate, and their benefit are judged to exceed the overall cost, they should be allocated. If resources are insufficient, the decision is made to either accept more risk or find more resources. In cases of personal safety, there is always some component of risk reduction that is inherently dependent on the person at risk and these measures need to be included in evaluating available resources.

Implementation of Risk Reduction Methods and Countermeasures

Once the resources are allocated, the entities and persons responsible for implementation are charged with that duty. The process of selecting the staff, vendors, or other parties that will implement the methods and countermeasures is undertaken. Then the projects are launched and managed to completion and placed into routine operation.

Evaluation of Risk Reduction Efficacy

After implementation, the risk reduction levels should be measured, and the methods and countermeasures are evaluated for their respective contributions to risk reduction. The cost of the methods and countermeasures are set against their effectiveness to see which ones provide the most protection for the money, time, and effort and accomplished the desired goals at the lowest overall cost.

Identifying and retaining only effective risk reduction methods is a critical step. If a method is not effective it not only allows more risk, but it also results in “security theater” that undermines public trust and often creates a backlash when the inefficacy is revealed. The ongoing challenge of risk management is that when done well, nothing happens, and one can be lulled into thinking there were no threats or that the counter measures taken were unnecessary. This often makes gaining or sustaining resources a challenge. Therefore, the avoidance of bad outcomes must be acknowledged and valued.

Monitor Active, Emerging, and Unaddressed Threats

A surveillance and survey process needs to be undertaken periodically to inform the threat management and risk reduction process. By monitoring what is happening vis a vis threats to public employees by querying both the people affected and various data sources, a jurisdiction can make sure their risk management plan can remain evergreen.

Periodic Revision and Re-evaluation of Threat Reduction Strategy

Using the efficacy and threat monitoring data, the threat management plan and strategy should undergo periodic reviewand updating. This should include level setting the risk tolerance of the leadership and evaluating availability of resources to ensure ongoing alignment.

Existing Resources and Laws

The process laid out above is practiced in all state and local jurisdictions and there are trained staff that would be able to apply their knowledge to the problem of public employee protection and threat and risk reduction. The Federal Government, some of these state and local jurisdictions, and private companies have done just that. The Federal Government has several laws and programs aimed at keeping public officials and employees safe. For example, the Election Threats Task Force surveyed and investigated threats against election workers and has begun prosecuting some of these cases. Here is a summary of their findings and responses:

- "The task force has reviewed over 1,000 contacts reported as hostile or harassing by the election community.
- Approximately 11% of those contacts met the threshold for a federal criminal investigation. The remaining reported contacts did not provide a predication for a federal criminal investigation. While many of the contacts were often hostile, harassing, and abusive towards election officials, they did not include a threat of unlawful violence.
- In investigations where the source of a reported contact was identified, in 50% of the matters the source contacted the victim on multiple occasions. These investigations accordingly encompassed multiple contacts. The number of individual investigations is less than 5% of the total number of reported contacts.
- The task force has charged four federal cases and joined another case that was charged prior to the establishment of the task force. There have also been multiple state prosecutions to date. The task force anticipates additional prosecutions in the near future.
- Election officials in states with close elections and postelection contests were more likely to receive threats. 58% of the total of potentially criminal threats were in states that underwent 2020 post-election lawsuits, recounts, and audits, such as Arizona, Georgia, Colorado, Michigan, Pennsylvania, Nevada, and Wisconsin."

The Congressional Research Service lists the following Federal laws that are relevant to election threats as well as threats in general:

- *18 U.S.C. § 115, which prohibits threats "to assault, kidnap or murder" federal officials, employees, or their family members with the "intent to impede, intimidate, or interfere with" the performance of official duties, or in retaliation for official duties;*
- *18 U.S.C. § 610, which prohibits intimidating or threatening federal employees to engage in or to not engage in "any political activity";*
- *18 U.S.C. § 876, which prohibits knowingly sending by mail "any communication ... addressed to any other person and containing any threat to kidnap any person or any threat to injure" and includes additional penalties for mailing threats to federal officials;*
- *18 U.S.C. § 1503, which prohibits "corruptly or by threats or force, or by any threatening letter or communication, influences, obstructs, or impedes or endeavors to influence, obstruct, or impede, the due administration of justice";*
- *18 U.S.C. § 1505, which prohibits the obstruction of justice, including by threats, for any proceeding before a U.S. agency or a congressional investigation;*
- *18 U.S.C. § 1512, which prohibits threatening or intimidating a witness in an official proceeding to withhold testimony, tamper with evidence, or prevent someone from reporting a federal offense to law enforcement;*
- *52 U.S.C. § 20511, which provides criminal penalties for any person, including an election official from, among other things, "knowingly and willfully intimidat[ing], threat[ening], or coerc[ing] or attempt[ing] to intimidate, threaten, or coerce any person for ... urging or aiding any person" in voting or registering to vote in a federal election; and*
- *52 U.S.C. § 10307, which prohibits persons acting under the color of law or otherwise from intimidating, threatening, or coercing any person for urging or aiding any person to vote or attempt to vote" or for enforcing the right to vote.*

Additionally a new law allows the Marshal of the Supreme Court to provide security to "any officer" of the bench if the Marshal deems it necessary. Supreme Court justices are currently covered by federal security protection under US Code. The new law extends those protections to immediate family members of the justices as well if the Marshal of the Supreme Court "determines such protection is necessary."

A reasonable line of inquiry regarding the list of statutes and new laws above is to see where states need, but do not have, comparable laws if federal jurisdiction cannot be established. Since the list above is not an exhaustive one of all the relevant laws that can be considered and applied to this problem, a thoughtful inventory and analysis of existing law is needed, which can be used to determine what advice to states could be generated regarding gaps in state laws.

This activity shows that beyond laws, there are numerous protection programs that can serve as models or inform us as to what needs to be improved to make public employees safer.

Congress has also acted on this topic for its own members and staff by allocating and allowing the use of funds for office and home security for members and their families.

Legislation in 2022 required the Senate Sergeant at Arms to create a "residential security system program" to protect senators in their home states and towns. Per the legislation, "the program is focused on assisting in mitigating increased risks to the physical security of senators' residences both in the District of Columbia and in their home states. The [budget allocation] provides a total of $2.5 million to be available until expended for the development and administration of a residential security system program." The spending bill also includes millions of dollars to bolster House member security. The legislation requires the U.S. House and Capitol Police to "enhance member protection including providing a security program for Congressional Leadership, expanding Dignitary Protection Division services, and expanding USCP field office presence." This would broaden Capitol Police protection in cities outside of Washington.

Further, according to Axios, "the Federal Election Commission ruled in March 2021 that members of Congress could use campaign funds to pay for bona fide personal security services. The decision came after the Capitol siege and as lawmakers of both parties dealt with persistent violent threats." Members are now spending thousands to hundreds of thousands of dollars on such security.

This includes the programs of the Marshal Service, the Supreme Court Police, the US Congress, the

Federal Protective Service of the Department of Homeland Security, the Capitol Police, FBI, Justice Department, State Department, State and Local Police, and many others. Private companies also have robust programs ranging from executive protection plans to safety programs for all employees. Grants have been given and used by several jurisdictions to improve security in the run up to the last election. Gleaning best practices from such programs, grants, and practices is also a task worth consideration to inform state and local government as to how best to improve their security for public employees.

Laws and programs that improve security of public employees that are informed by a robust security planning and risk mitigation process is what is needed to rise to the level of this problem in our society. Policy makers and government managers need to know what the viable threats are, how to address them, know what works, and allocate resources to meet our level of risk tolerance. Next, they can consider what kinds of countermeasures and methods could be considered as part of a study process, laws, and resource allocations.

Countermeasures and Methods to Be Considered as Part of a Law and Policy Process

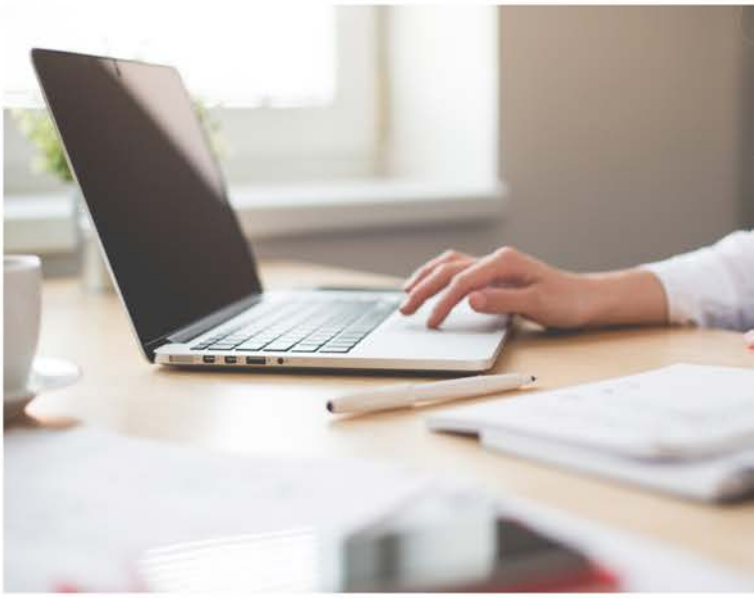
A best practice in risk reduction is what is called "security-in-depth." Also known as layered protection and defense-in-depth, security-in-depth is a concept that means placing a series of progressively more difficult obstacles in the path of an aggressor. These obstacles are often referred to as lines of defense. What this means is that one should use a variety of risk reduction methods and countermeasures to avoid single points of failure and to make the security response itself more robust and resilient.

One thing to avoid in pursuing security-in-depth is "security theater" as noted above. Wikipedia defines this as "the practice of taking security measures that are considered to provide the feeling of improved security while doing little or nothing to achieve it." The article goes on to say that "by definition, security theater provides no security benefits (using monetary costs or not), or the benefits are so minimal it is not worth the cost." And further notes that critics "have argued that the benefits of security theater are temporary and illusory since after such security measures inevitably fail, not only is the feeling of insecurity increased, but there is also loss of belief in the competence of those responsible for security."

Redacting the very public and easily discovered fact of the addresses of public employees is security theater. It's widely known and acknowledged that one can find a person's address by numerous means. Further, the dark web also provides cheap complete profiles of persons gleaned from hacked data, data breaches, malware, apps with loose privacy policies, and data from many, many sources in common circulation. For example, a recent collection of breached data comprising 26 billion records totaling 12 terabytes of information was made available on the dark web in January of 2024.

It is also relevant to consider that those who are willing to go beyond the stage of thought to actual action to harm, harass, threaten, and stalk a public employee are not in any way likely to be deterred by weak security theater level measures such as redacting addresses.

The argument is often made that if a particular security or safety measure prevents even one harm, it is worth it. This is a clear fallacy as we do not practice this approach in allocating government resources or regulating anything. Common sense tells us to balance competing priorities. Spending on ineffectual security theater diverts resources from effective measures that would address real threats and reduce harm. The tactic of redacting addresses in public records has substantial direct and indirect costs that make such redactions a badly imbalanced approach. There are better ways to protect public employees.



METHODS & COUNTERMEASURES

The following is a list of possible methods and countermeasures that have been deployed in public and private sector security plans that have proven to be effective. These could be applied alone and in various combinations and at various levels of effort depending on the threat and what works best against it. Using combinations of these would create lines of defense and security-in-depth that would be deployed in alignment with the process described above for threat management.

- **Identity, Reputation, and Credit Management, Monitoring, and Repair Services**
  - This can be considered as a new and necessary employee benefit for all or for selected employees deemed at higher risk
- **Electronic Surveillance, Monitoring, and Threat Detection**
  - This includes video surveillance, social media monitoring, audio sensors, chemical sensors, AI programs, computer network monitoring, and device security.
- **Call Screening Software and Services**
- **Security Personnel**
  - This includes those routinely assigned to locations as well those who can be deployed to where the threat may be realized and when the threat level for a person or group of persons goes up
- **Physical Barriers**
- **Cybersecurity Training and Services**
- **Personal Safe Rooms and Panic Buttons**
- **Self-Defense Training**
- **Self-Protection Devices and Weapons**
- **Safety Procedures and Protections**
  - For example, safe words, pattern variance, having an electronic way to monitor home entrances, not answering the door directly when a stranger is present, and so on
- **Civil Legal Processes and Support**
  - Public employees may need assistance to use the laws available to protect themselves and pursue those to have harmed them or seek to harm them
- **Protective Orders**
- **Law Enforcement and Prosecutorial Personnel and Policy Priorities**
- **New Criminal and Civil Laws, Rules, and Policies (as discussed above)**
- **"Safe at Home" Programs**
  - For victims of domestic violence, witnesses, and others under active threat.
  - These programs provide an alternative mailing address for those persons who have been adjudicated as needing this form of enhanced protection.
- **Allowing persons with government sanctioned alternative identities in special cases such as for persons in witness protection, undercover agents, and national security personnel.**

CONCLUSION

Along with beneficial commercial and transactions uses, there are many uses for address information that is essential to citizen and press oversight of government. For example, if an elected official owns property and the roads in front of the property receive improvements and maintenance that are outside normal procedures, a citizen, or any other party, including news organizations, should be free to make an inference that the elected official was receiving special treatment, or such property otherwise benefited in a manner that others have not. If a person running for office where there is a residency requirement is found to have connections to addresses and taxation outside of the jurisdiction, it could be inferred that the candidate may not qualify for the office sought or that their residency is a legitimate issue for voters to consider when voting. Press investigations and citizen investigations using address data have uncovered issues such as graft, corruption, ethics violations, and voter fraud just to name a few. The National Freedom of Information Council and 25 state freedom of information coalitions have issued a letter opposing over-broad address redaction for public employees and pointing out the beneficial uses of such addresses.

We lack any solid evidence that informational obscurity on addresses will deter a determined bad actor who has the capacity for violence and harmful behavior. We know that public employees are facing a more hostile and violent subset of the public that is willing and able to harm them. We must take this threat seriously and match the threats with processes, programs, and laws that will reduce and prevent risks, deter bad actors, and apprehend and punish those who break the law while targeting public employees. A longer and more complete set of actions to enhance public employee safety that goes beyond a single weak and ineffective redaction concept to an all-threats, security-in-depth approach is what the times demand and what public employees deserve.

Did You KNOW?

IN A SINGLE YEAR PUBLIC RECORDS PLAY A KEY ROLE IN THE:

- Purchase of over 6 million residential homes
- Sale of over 17 million cars
- Notification of nearly 53 million auto recalls
- Issuance of over 21 million passports and travel cards
- Creation of quality-of-care reports protecting over 7 million children (under age 5) in day care and over 8 million adults receiving long-term care
- Detection of fraud and fair underwriting for 291 million life, 167 million health, and 234 million car insurance policies
- Checking the performance, quality, and stability of 6,800 banks, 13,000 credit unions, and 1,000 saving and loan institutions

CSPRA

CSPRA works to inform the public and policy makers about the beneficial commercial uses of public records and promote a balanced discussion of the role of public records in an information-based economy.

Society Benefits from the LEGITIMATE USE OF PUBLIC RECORDS

The Everyday VALUE of Public and Private Records WORKING TOGETHER

Consumers and government benefit from the combination of public and private records systems. Together, these systems produce value-added services, including: protection of children and seniors, lending, oversight of government, child support enforcement, improved newsgathering and economic forecasting. Public and private records systems working alone do not provide an equivalent capacity to enhance public safety, facilitate commerce and reduce government costs and inefficiencies.

The use of PUBLIC RECORDS in our DAILY LIVES

BUYING OR SELLING A HOME:

- Evaluate the mortgage applicant and validate the funds
- Identify the payment of property taxes
- Conduct a lien search
- Produce a clear title
- Discover any pending litigation against the seller
- Discover environmental hazards
- Verify easements or encroachments
- Find neighborhood ratings (criminal activity, school performance, walkability)

CHOOSING A CARE PROVIDER:

- Verify provider's credentials, including background checks
- Obtain public health and safety reports
- Determine providers public assistance programs
- Obtain a care provider report card

BUYING A CAR:

- Conduct credit check for a loan
- Identify recalled vehicles
- Confirm proper titling
- Find safety and fuel consumption ratings
- Reveal crash and repair history
- Align insurance rates to driver behavior

ENABLING COMMERCE:

- Open a bank account
- Apply for credit
- Reduce identity theft crime
- Help consumers know where their purchases come from
- Improve supply chain efficiency for businesses
- Identify and prevent money laundering
- Allow investors to better value stocks and bonds

GETTING A JOB:

- Perform background check
- Verify licenses and credentials
- Confirm work eligibility under the law

TRAVELING ABROAD:

- Obtain a passport or travel visa
- Prove residency
- Identify country immunization and public health requirements
- Access terrorism and safety alerts

KEEPING PEOPLE SAFE:

- Arrest criminals
- Reduce consumer fraud
- Improve access to the justice system
- Publicize known offenders
- Protect vulnerable people