TAB 8

City of Palmetto Agenda Item

Meeting Date

09/10/12

Presenter: Rick Wells **Department:** Police Department

Title: Dual Authentication and Single Sign-On for Police Department

The City of Palmetto Police Department, in order to comply with the Criminal Justice Information Systems Security Policy (CJIS), would like to contract with Imprivata for implementation of an Advanced Authentication (AA) solution. Advanced Authentication is the term describing added security functionality, in addition to the typical user identification and authentication of login ID and password (such as: biometric systems, public key infrastructure (PKI), smart cards, software tokens, hardware tokens, or Risk-based Authentication). CJIS policy, Version 5.0 dated January 2011(CJIS 7.3.2.3.1 Definitions and Policies for Advanced Authentication) , outlines certain security requirements for any law enforcement agency that accesses criminal justice information (CJI) through the State or FBI CJIS systems. The City of Palmetto Police Department is one of those law enforcement agencies and, therefore, must comply with the CJIS policy. The deadline to implement this technology is 2013 and CJIS has inquired about how we plan to meet this timeframe.

Because any terminal within any the City of Palmetto Police Department facility has the capability of accessing criminal justice information, all laptops, terminals, and servers will have a 'two-factor' or Advanced Authentication. Additionally, laptops removed from the premises or vehicle must meet Advanced Authentication requirements (CJIS Policy, Section 7.2.4 (b)). Furthermore, the CJIS policy requires all systems that allow access to CJI to have complex passwords in order to ensure a higher level of information security.

Imprivata is the only vendor that provides a centrally managed Authentication and Single Sign-On solution (not requiring any administration at the workstation level). Imprivata has designed a proprietary agent to support all applications, including a specific agent for the deployment within Windows Terminal Services Environments. In addition to performing Advanced Authentication, the CJIS policy also requires each agency to demonstrate an audit trail of all users and systems that allow for CJI access. Imprivata is the only Advanced Authentication vendor that can provide integrated audit reporting at the application level. All other authentication vendors only allow this level of reporting at the network level only, and therefore would leave out the data within the USA CAD and NCIC/FCIC applications. Imprivata's Advanced Authentication solution is currently being used by several other Florida Agencies (see attached list).

Staff feels that it is in the Department's best interest to utilize a known vendor with a proven solution and believe Imprivata is the sole source vendor that can provide the solution that we need. We have attached a sole source letter that further supports the sole source justification (see attached letter).

The total estimated cost to implement the solution is approximately $29,000 and includes all hardware, software, training and the 1st year of maintenance (see attached quote). Approximately $9,000 in impact fees will be used to help fund the expense. The balance of $20,000 is budgeted in the FY 2013.

Budgeted Amount:	$29,440	**Budget Page No(s):**		**Available Amount:**	$29,440	**Expenditure Amount:**	$29,440

Additional Budgetary Information: $9,000 of impact fees and $20,000 from FY 2013 operating budget.

Funding Source(s):	521	**Sufficient Funds Available:**	☒ Yes ☐ No	**Budget Amendment Required:**	☐ Yes ☒ No	**Source:**	

City Attorney Reviewed:	☒ Yes ☐ No ☐ N/A	**Advisory Board Recommendation:**	☐ For ☐ Against ☒ N/A	**Consistent With:**	☐ Yes ☐ No ☒ N/A	

Potential Motion/ Direction Requested:	Motion to approve and authorize staff to purchase the dual authentication/single sign-on technology from sole source vendor Imprivata via the distributer Computer Discount Warehouse Government (CDW-G) in the amount of $29,244.
Staff Contact:	Rick Wells
Attachments:	List of other agencies using Imprivata, Sole Source letter, Quote

State of Florida Imprivata Customers

Florida Highway Patrol
Department of Environmental Protection
Department of Transportation Motor Carriers Compliance
Osceola County Sheriff's
Palm Beach County Sheriff's
Polk County Sheriff's
Nassau County Sheriff's
Alachua County Sheriff's
City of Key West Police Dept.
City of Homestead Police Dept.
City of Aventura Police Dept.
City of Delray Beach Police Dept.
City of Sarasota
City of Miami Beach (including the Police Dept.)
City of Coral Gables Police Dept.
City of Boca Raton Police Dept.

We have many other projects in various states of completeness all over the State.

CDW·G

CDWG.com | 800.594.4239

OE400SPS

SALES QUOTATION

QUOTE NO.	ACCOUNT NO.	DATE
CWFX710	10134579	8/9/2012

BILL TO:
AUBREY DRUMMOND
516 8TH AVE W

Accounts Payable
PALMETTO , FL 34221-5122

Customer Phone #941.723.4570

SHIP TO:
CITY OF PALMETTO
Attention To: AUBREY DRUMMOND
516 8TH AVE W

PALMETTO , FL 34221-5122
Contact: JIM FREEMAN 941.723.4570

Customer P.O. # IMPRIVATA QUOTE

ACCOUNT MANAGER	SHIPPING METHOD	TERMS	EXEMPTION CERTIFICATE
DAN HOGAN 866.537.4615	DROP SHIP-GROUND	MasterCard/Visa Govt	GOVT-EXEMPT

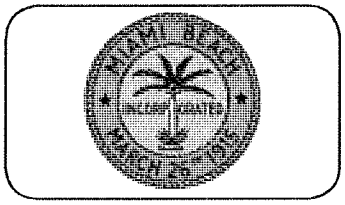
QTY	ITEM NO.	DESCRIPTION	UNIT PRICE	EXTENDED PRICE
2	2119135	IMPRIVATA ONESIGN NEW VIRTUAL APPLIA Mfg#: NEW-VIR-APP Contract: MARKET	0.00	0.00
30	2041202	IMPRIVATA UPEK EIKONTOUCH 500 USB FP Mfg#: HDW-UPEK-TCRF1S Contract: National Joint Powers Alliance 111309-CDW	115.00	3,450.00
50	1786512	IMPRIVATA ONESIGN FASTPASS 25-1499U Mfg#: FBID-25 Contract: National Joint Powers Alliance 111309-CDW Electronic distribution - NO MEDIA	7.00	350.00
50	1816939	IMPRIVATA ONESIGN SSO/AM 50U NEW Mfg#: SSO/AM-50-USR Contract: National Joint Powers Alliance 111309-CDW	167.00	8,350.00
50	1784898	IMPRIVATA ONESIGN SSPW MGT 25-1499U Mfg#: SSPW-25 Contract: National Joint Powers Alliance 111309-CDW Electronic distribution - NO MEDIA	7.00	350.00
12	2395626	IMPRIVATA ONESIGN PREM-V MNT Mfg#: SUPV25 Contract: National Joint Powers Alliance 111309-CDW	246.00	2,952.00
1	1695118	IMPRIVATA 2-DAY ONSITE GEN BOOT CAMP Mfg#: TR-BTCMP-GEN Contract: National Joint Powers Alliance 111309-CDW	4,541.00	4,541.00
2	2035003	IMPRIVATA-ONESIGN SVCS INSTAL/CONFIG Mfg#: TR-INSTALL-ONSITE Contract: National Joint Powers Alliance 111309-CDW Electronic distribution - NO MEDIA	2,271.00	4,542.00
3	2035005	IMPRIVATA-ONESIGN SVCS INSTAL/CONFIG Mfg#: TR-INSTALL-REMOTE Contract: National Joint Powers Alliance 111309-CDW Electronic distribution - NO MEDIA	1,635.00	4,905.00

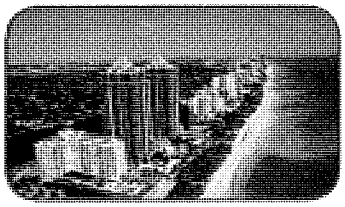
SUBTOTAL	29,440.00
FREIGHT	0.00
TAX	0.00

US Currency

TOTAL ➧ 29,440.00

City of Miami Beach Cuts Overhead and Improves Security with Imprivata OneSign®





INTRODUCTION

Government agencies face a paradox: serving the public requires unimpeded access to disparate software applications, while maintaining information security requires ever more complex login routines, with growing regulatory oversight. And with shrinking state and local tax revenues, government agencies have fewer resources for providing high levels of public services.

Such was the dilemma for the City of Miami Beach, a municipality with a year-round population of about 90,000 that regularly triples to 300,000 or more.

THE BUSINESS CHALLENGE

"Managing multiple passwords with different complexity rules was getting out of hand for certain departments," says Nelson Martinez Jr., Systems Support Manager for the City of Miami Beach. "People were writing down passwords in PDAs or notebooks and whipping out pieces of paper to remember passwords." Not surprisingly, reset requests were jamming helpdesk lines as well.

Beyond password consolidation and single sign-on, the challenge was finding a solution compatible with the specialized niche applications that are ubiquitous in local government environments. Architecturally, such applications are often atypical or outdated, creating multiple implementation headaches.

With password hurdles mounting, Martinez began looking for single sign-on (SSO) options late in 2005. "About that time I received a flyer in the mail from Imprivata for a purpose-built appliance called Imprivata OneSign®," he recalls. "I'd never heard of it, but an appliance-based product caught my eye."

THE IMPRIVATA ONESIGN SOLUTION

Martinez researched multiple available SSO offerings, including Imprivata OneSign. Says Martinez, "We wanted something that would kill multiple birds with one stone —from reducing reset requests to assisting with multiple profiles for niche apps and legacy systems," Martinez emphasizes. "We also wanted self-service features that helped users of all types from all divisions within the city government gain confidence and have a better experience. During the hands-on testing, it was clear that Imprivata OneSign fit the bill."

In addition, Miami Beach was impressed with Imprivata OneSign's built-in capability to integrate biometric devices. "We decided to deploy fingerprint readers in IT initially, and then offered them to departments throughout the city," says Martinez.

The initial Imprivata OneSign implementation in mid-2006 included niche applications, legacy systems, and fingerprint readers. "Although the Imprivata OneSign appliance was configured within hours, we were completely up and running in under two weeks," Martinez says. "Then we rolled out Imprivata OneSign to users in a phased approach. We posted an FAQ on our intranet and conducted hands-on training to achieve buy-in. We finished the entire rollout in less than four months and it's worked great ever since."

ORGANIZATION

- Employees: >1800

INDUSTRY

- Local government (including police, fire and code enforcement)

APPLICATIONS

- Niche and legacy government applications; law enforcement applications accessing federal crime database

CHALLENGES

- Heterogeneous environment with niche applications
- Difficulty enforcing password policies
- High volume of helpdesk calls for password resets

RESULTS

- Reduced helpdesk calls
- Compliance with FBI CJIS requirements for authentication
- Enhanced security of constituent data

BEFORE IMPRIVATA ONESIGN	AFTER IMPRIVATA ONESIGN
Multiple passwords with different complexity rules were becoming unmanageable and affecting productivity for certain departments	SSO improves user productivity with one login across many applications - 1,800 users SSO-enabled
Excessive helpdesk calls for password resets and after-hours calls	Self-service password management eliminates reset calls to the helpdesk, reducing administrative overhead
Difficulty demonstrating access security for constituent data	Fingerprint biometrics, audit and reporting aid security and compliance

THE RESULTS

Imprivata OneSign quickly met the city's initial needs of reducing password reset requests. According to Martinez, "Now supporting 1,800 users, Imprivata OneSign has slowed password reset requests to a trickle. We need fewer helpdesk resources to support our staff. And we rarely get any reset calls in the middle of the night anymore."

But the benefits have extended far beyond the time savings of reducing password resets. In the years since initial deployment, the City of Miami Beach has reaped additional benefits from centralized application access control with strong authentication capabilities.

- **CJIS compliance:** The FBI requires law enforcement agencies connecting to the Criminal Justice Information Services (CJIS) systems to use unique IDs and strong passwords by 2010, and advanced authentication by 2013. With Imprivata OneSign, City of Miami Beach has been able to enforce complex passwords and implement fingerprint biometrics, meeting the second requirement ahead of the 2013 deadline.
- **Audit readiness**: Using Imprivata OneSign's extensive audit and reporting capabilities, the City of Miami Beach can immediately demonstrate to auditors that they track all application access and enforce authentication and access policies. According to Martinez, "Once auditors see what the OneSign solution does, they don't have to ask many additional questions—our experience has been very positive."
- **Disaster resilience**: "We're moving toward an emphasis on business continuity where everything at our co-location is hot, spinning, and available," says Martinez, who represents the City of Miami Beach on a state-wide task force that is adapting corporate enterprise standards for government use. "Our distant hot site will allow the city to keep working even if our data center goes, and OneSign will definitely play a role."

At an organization charged with serving the public and delivering taxpayer value, Imprivata OneSign has proven an excellent fit, Martinez emphasizes. "Imprivata OneSign has improved productivity throughout city departments because people aren't sitting around waiting for a simple password reset, and has helped us manage audits and new compliance requirements," he says. "They really see the value and flexibility the solution provides to their business unit, especially those that are 24 hour operations."

"Imprivata OneSign has improved productivity throughout city departments because people aren't sitting around waiting for a simple password reset, and has helped us manage audits and new compliance requirements. They really see the value and flexibility the solution provides to their business unit, especially those that are 24 hour operations."

– Nelson Martinez Jr., Systems Support Manager City of Miami Beach

1 877 ONESIGN | 1 781 674 2700 | www.imprivata.com

MKT-SS-COMB-Ver2-03-2011

imprivata®

September 2, 2012

To Whom It May Concern:

The City of Palmetto Police Department, in order to comply with the Criminal Justice Information Systems Security Policy (CJIS), has consulted Imprivata to assist in a potential implementation of an Advanced Authentication (AA) solution.

Advanced Authentication is the term describing added security functionality, in addition to the typical user identification and authentication of login ID and password, such as: biometric systems, public key infrastructure (PKI), smart cards, software tokens, hardware tokens, or Risk-based Authentication. (CJIS 7.3.2.3.1 Definitions and Policies for Advanced Authentication)

Background:
The CJIS policy, Version 5.0 dated January 2011, outlines certain security requirements for any law enforcement agency that accesses criminal justice information (CJI) through the State or FBI CJIS systems. The City of Palmetto Police Department is one of those law enforcement agencies and, therefore, must comply with the CJIS policy.

Because any terminal within any the City of Palmetto Police Department facility has the capability of accessing criminal justice information, all laptops, terminals, and servers will have a 'two-factor' or Advanced Authentication. Additionally, laptops removed from the premises or vehicle must meet Advanced Authentication requirements (CJIS Policy, Section 7.2.4 (b)).

Furthermore, the CJIS policy requires all systems that allow access to CJI to have complex passwords in order to ensure a higher level of information security. The guidelines are:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the Userid.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

As a result of the complex password policy a significant burden is placed on the CJI users/officers as these passwords are often forgotten, resulting in a user account lockout or helpdesk call, significantly delaying or even preventing an officer from accessing CJI and thus being able to perform his/her duties. To combat this, users will often write passwords down or share them with others, which in addition is not best practice for information security, would be non-compliant with the CJIS policy.

Therefore, the City of Palmetto Police Department will implement an Enterprise Single Sign-On solution to provide ease of access to CJI and maintain the proper level of security required to comply with CJIS. Enterprise Single Sign-On is a defined as a solution that only requires a user entering authentication one-time to Windows, and subsequent authentications to other systems are automated via the software without requiring manual user intervention.

Project:

The City of Palmetto Police Department plans to implement Advanced Authentication via fingerprint biometrics for all of its laptops within its vehicles, as well as for workstations internal to the office that access CJI, such as PC's within the squad room. The City of Palmetto Police Department also plans to implement an Enterprise Single Sign-On solution that will encompass all systems that allow access to CJIS.

System Requirements:
The City of Palmetto Police Department has the following requirements for the project:

- The solution must not change or modify the Active Directory Schema
- The solution must support a broad variety of strong authentication modalities including finger biometrics plus password and hardware or software tokens plus password, and question and answer
- The solution must integrate with all applications for single sign on, as well as be managed centrally or at the network level
- The solution must provide an audit reporting system on network and application access

Listed below is a justification to support each stated requirement and justification of sole sourcing:

1) The City of Palmetto Police Department must implement Advanced Authentication immediately due to the CJIS policy's rule which requires any agency that has made an upgrade or replacement of any hardware or software that provides access to CJI since 2005. Due to the compelling timeline of this rule, the City of Palmetto is requiring that any solution not require any Active Directory schema change as this would significantly delay the time to implement as well as expose the network to more risk, and risk the result of a failing audit.

   Imprivata is the only biometric authentication solution that does not store biometric information within Active Directory, thus not requiring schema modification. Imprivata will provide a self-contained, centrally managed separate user database thus ensuring quick deployment and completion within the City of Palmetto Police Department's timeline.

2) Biometrics is the recommended primary authentication solution as it reduces the risk of compromise by a stolen or lost smartcard, proximity card or token, thus not requiring the user to carry any extraneous device. If biometrics are deemed to be unavailable at the time of CJI access, the City of Palmetto must have a viable alternative to meet CJIS guidelines to prevent a situation where an officer would be restricted from CJI access. Therefore, a solution that encompasses multiple forms of authentication is required, such as hardware or software tokens, and a question and answer method. Imprivata is the only vendor that supports biometrics, tokens, and question and answer.

   Imprivata is the only Authentication Solution that supports finger biometrics, all methods of tokens, and question and answer. Imprivata is also the only Authentication solution that allows the dispersal of such methods at the user, group, or Active Directory OU level, therefore allowing the flexibility to truly control how each department/group/team/user accesses data.

3) The City of Palmetto Police Department utilizes a number of applications including USA Computer Aided Dispatch (CAD) and National Crime Information Center NCIC and Florida Crime Information Center FCIC. USA CAD is the primary law enforcement application and NCIC/FCIC is the federal inspection system. Allowing single sign-on ensures that an officer would not have to worry about a forgotten password preventing him or her from CJIS access. These applications are hosted centrally within the network via Windows Terminal Services and therefore are not locally installed on its laptops. Due to this, the Advanced Authentication and Single Sign-On solution must be managed centrally.

   In order to integrate with centrally hosted applications, the solution must be managed centrally and support Windows Terminal Services or like environments. Any solution that requires administration at the workstation level will cause incompatibility or significantly delayed times of implementation, support and maintenance, and upgrading thus jeopardizing the City of Palmetto's ability to implement or support it.

   Imprivata is the only vendor that provides a centrally managed Authentication and Single Sign-On solution; not requiring any administration at the workstation level. Imprivata has designed a proprietary agent to support all applications, including a specific agent for the deployment within Windows Terminal Services Environments.

4) In addition to performing Advanced Authentication, the CJIS policy also requires each agency to demonstrate an audit trail of all users and systems that allow for CJI access. Therefore, a system must be able to provide access of:

   a. Who accessed the network

   b. What was the method of authentication

   c. What workstation was the CJI accessed on

   d. What applications were accessed

   Imprivata is the only Advanced Authentication vendor that can provide integrated audit reporting at the application level. All other authentication vendors only allow this level of reporting at the network level only, and therefore would leave out the data within the USA CAD and NCIC/FCIC applications.