FLORIDA CYBERSECURITY TASK FORCE MEETING
Tuesday, December 03, 2019, 10:00am – 12:00pm
Student Academic Success Center #100
11200 SW 8th, Miami, FL 33174

TABLE OF CONTENTS

1. Agenda & Presenter Biographies
2. October 22nd Meeting Minutes
3. Elections Update Materials
4. State Governments at Risk Cybersecurity Presentation by NASCIO
5. Cybersecurity Presentation by Black Knight
Meeting Notice & Agenda:
Florida Cybersecurity Task Force

Date & Time:
December 3, 2019
10:00 am

Location:
Florida International University
Student Academic Success Center #100
11200 SW 8th Street
Miami, FL 33174

I. Call to Order

II. Roll Call

III. Welcome by DMS Secretary Satter

IV. Approval of Minutes from Organizational Meeting

V. Discussion on Path Forward

VI. Presentation: Elections Update
Laurel Lee, Secretary, Florida Department of State

VII. Presentation: State of our Cybersecurity Infrastructure
Doug Robinson, President, National Association of State Chief Information Officers

VIII. Panel Discussion: Local Government Cybersecurity Challenges and Opportunities
Ray Desjardins, Chief Information Officer, Charlotte County
Ramin Kouzehkanani, Chief Information Officer, Hillsborough County
Archie Satchell, Chief Information Officer, Palm Beach County

IX. Presentation: Cyber Threats and Opportunities
Mike Housch, Chief Information Security Officer, Black Knight

X. Group Discussion

XI. Public Testimony

XII. Adjournment
Presenter Biographies

Laurel Lee
Secretary of State
Florida Department of State

Secretary of State Laurel M. Lee was appointed by Governor Ron DeSantis as Florida’s 36th Secretary of State and began serving in February 2019. Secretary Lee previously served as the Circuit Court Judge in Florida’s Thirteenth Judicial Circuit in Hillsborough County. She was appointed to the Circuit Court by Governor Rick Scott in 2013 and re-elected without opposition in 2014.

During her time as Circuit Court Judge, Secretary Lee presided in the Circuit Civil Division, the Civil Appellate Division and the Domestic Relations Division. She was also a member of the Florida Supreme Court’s Steering Committee on Family and Children in the Courts and the Florida Supreme Court’s Commission on Trial Court Performance and Accountability.

Prior to serving as a Judge, Secretary Lee was an Assistant United States Attorney in the Middle District of Florida where she initiated and prosecuted a wide range of criminal offenses. Her special responsibilities included serving as the Violence Against Women Act Coordinator, the coordinator for the interagency Bankruptcy Fraud Working Group, and as the lead prosecutor for the Child Prostitution Task Force.

Before becoming a federal prosecutor, Secretary Lee worked as an Assistant Federal Public Defender in the Middle District of Florida and as a judicial law clerk to United States District Court Judge James S. Moody, Jr. She previously practiced law at Carlton Fields, P.A. in Tampa where she specialized in antitrust and complex business litigation.

In addition to her extensive legal and judicial experience, Secretary Lee has been an active member of her community where she has served on a variety of local boards and volunteered with numerous community organizations, including as a pro bono attorney through the Bay Area Legal Services Domestic Violence Assistance Program.

Secretary Lee received her Bachelor’s Degree and a Juris Doctorate from the University of Florida, where she was a member of Florida Blue Key. She was inducted into the University of Florida Hall of Fame in 1999.

Secretary Lee is married to Florida State Senator Tom Lee and they have three children, Regan, Brandon and Faith.
Doug Robinson is the president of the National Association of State Chief Information Officers (NASCIO). Before he was elected as the president, Mr. Robinson served as Executive Director of the NASCIO for over 16 years.

Doug is a frequent speaker, panelist, author and recognized national expert representing state CIOs, policy issues, priorities and trends in state government IT. In 2012, he was elected as a Fellow of the prestigious National Academy of Public Administration. Doug represents NASCIO on several national councils, boards and advisory committees. Among his recognitions, in 2015 he received the Advocacy for Archives award presented by the Council of State Archivists. In 2006, he was named to Government Technology magazine’s top 25 Doers, Dreamers and Drivers in public sector information technology.

His career spans over thirty-seven years in public sector information technology including positions in state government, higher education and IT consulting. Prior to joining NASCIO he served as Executive Director in the Governor’s Office for Technology, Commonwealth of Kentucky. As a senior IT executive in the state CIO office, he led IT strategic planning, enterprise architecture, policy and research initiatives for state government.

His previous leadership positions in state government include Executive Director of the Kentucky Information Resources Management Commission and Executive Director of the Kentucky Office of Geographic Information. For fifteen years, he served in a university public service and technical assistance role with NASA’s Technology Applications Center in the Martin School of Public Administration at the University of Kentucky.

Doug holds a BA from Maryville College in Tennessee and a Master of Public Administration (MPA) with a concentration in science, technology and public policy from the University of Tennessee.
Ray Desjardins
Chief Information Officer
Charlotte County

Ray Desjardins is an experienced IT manager with over 28 years of experience in IT operations, from desktop support to server administration. Mr. Desjardins currently serves as the senior division manager for the Charlotte County Board of County Commissioners.

He is a certified Government Chief Information Officer (CGCIO) from the John Scott Dailey Florida Institute of Government (FIOG) at Florida State University.

Mr. Desjardins is working to establish stronger collaboration both within and outside of local government, and to develop public/private partnerships to further economic development.

President of Florida Local Government Information Systems Association (FLGISA).

Ramin Kouzehkanani
Chief Information and Innovation Officer
Hillsborough County

Ramin Kouzehkanani is a Chief Information Officer with significant years of experience in leading large organizations in both public and private sectors. Extensive experience in management and technology consulting, transformation of service delivery systems, statistical analysis, and Lean Sigma.

Ramin has shown demonstrated success in aligning technology departments, platforms, and budgets with overall organizational goals and objectives. Launched 3Advisory, LLC, a Health & Human Services consulting and advisory firm to focus on assisting states and national child-welfare agencies in their efforts to implement Federal rules through the establishment of strategic roadmaps for interoperability of data systems and processes, data exchanges, and predictive modeling in Child Welfare and Human Services.

Served in Florida Governor Crist’s Administration until 2011 and continued service in Florida Governor Scott’s Administration until September of 2011. Also served as senior advisor to Assistant Secretary George Sheldon at the United States Department of Health and Human Services Administration for Children & Families, the State of Illinois Department of Children & Family Services, and the State of Florida Department of Children and Families’ Community-Based Care agencies.

Ramin received a double major bachelor’s degree in Computer Science and Statistics from the University of Brighton and a Master of Business Administration from Western New England University.
Archie Satchell is the Chief Information Officer of Information Systems Services (ISS) Department for Palm Beach County, FL, a position he has held since 2018. Archie previously served as the Deputy Chief Information Officer from 2017 to 2018, as ISS Application Services Division Director from 2006 to 2017, as Senior Manager for Software Applications development from 2001 to 2006, and various software development positions from 1991 to 2001 with Palm Beach County.

Palm Beach County ISS manages a regional fiber optic network, develops and maintains an extensive inventory of in-house applications, provides a centralized GIS platform, and provides enterprise support for desktops, servers, and mobile devices. Additionally, the County provides network and application hosting services for numerous collaboration partners, including local governments, education institutions, and non-profit organizations within and outside Palm Beach County. Palm Beach County has been ranked previously as the #1 “digital county” among all large U.S. counties by the Center for Digital Government and has been consistently ranked among the top 10 counties nationwide over the past several years. Palm Beach County has recently completed a large-scale project deploying a Unified Communications platform which serves over 10,000 employees located in more than 470 facilities spread throughout the county.

Archie graduated from Northwood University with a Bachelor of Business Administration degree.

Mike Housch is the Chief Information Security Officer for Black Knight. He is responsible for establishing and maintaining the enterprise information security vision, strategy, and program, ensuring information assets and technologies are adequately protected.

Mike passionately leads global teams that drive operational security activities, vulnerability management, architecture, engineering, incident response, forensic operations, eDiscovery, litigation support, security governance, and regulatory audit oversight.

Mike has a longstanding career serving in the CISO capacity of more than fifteen years and continues to drive change within Black Knight through innovation and effective management of the program.
I. Call to Order

Lieutenant Governor Jeanette Nuñez called the meeting to order at 3:00 p.m. and provided introductory remarks. Lieutenant Governor Nuñez confirmed that the meeting notice was published in the Florida Administrative Register (FAR) on October 16, 2019. Future meeting notices will be published in the FAR and on the Department of Management Services (DMS) website. The Chair thanked the Governor and Legislature for their work in establishing the Task Force and their commitment to improve the security of the state.

II. Roll Call

Members in attendance: Chair and Lieutenant Governor Jeanette Nuñez, Sandro Alvarez, Michael Delgado, Shane Desguin, Dr. Eman El-Sheikh, Bernard Kelly, Melinda Miguel, Ben Miron, Jared Moskowitz, Jason Raymond, Linda Reid, Byron Shinn, Jeffrey Sturman, and Thomas Vaughn.

Excused Absence: Mike Phillips

Vacant Seat: State CIO (not yet appointed)

The Chair confirmed there was a quorum of the Task Force.

Lieutenant Governor Nuñez thanked the sponsors of HB 5301, including Representative Williamson who attended the meeting. Lieutenant Governor Nuñez emphasized the importance of the work the Task Force will undertake.

III. Member Introductions

Lieutenant Governor Nuñez asked for each member to provide a brief introduction. Each member briefly discussed their respective professional experience and history with information technology and cybersecurity issues. Each member expressed their appreciation and honor for being appointed to serve on the Task Force.

IV. Review and Adoption of Task Force Rules

Lieutenant Governor Nuñez referenced the materials in Tab 1 of meeting materials.

Absent any questions from the Task Force, Melinda Miguel made a motion to approve the Task Force Rules in the meeting materials and was seconded by Jeffrey Sturman. The Task Force Rules were approved unanimously by the Task Force.
V. Presentation: Scope, Purpose, and Responsibility of the Task Force

Lieutenant Governor Nuñez introduced Cody Farrill, who made the presentation. Cody Farrill described DMS’ role and a summary of HB 5301. Material in Tab 2 of the meeting materials, including the required objectives of the Task Force, was referenced. There was also discussion of the strategic topics that will be covered at each meeting, which will help ensure the Task Force is able to make recommendations in a timely manner.

VI. Presentation: State of our Cybersecurity Infrastructure

Thomas Vaughn provided an overview of the state cybersecurity infrastructure, referencing resources in Tab 3 of the meeting materials. There was discussion of the Florida Cybersecurity Standards, Rule Chapter 60GG-2, and other state strategic security measures, security operations, and other germane resources.

VII. Presentation: Government in the Sunshine Training

Chasity O’Steen presented the Sunshine Law and public records training using the resources in Tab 4 of the meeting materials.

VIII. Other Business & Proposed Meeting Schedule

Cody Farrill reviewed the proposed meeting schedule for the Task Force moving forward. Lieutenant Governor Nuñez encouraged the members to reach out to Cody Farrill if they have any requests or scheduling time constraints.

IX. Public Testimony

Lieutenant Governor Nuñez opened the floor for any public comment for those in attendance and on the phone. There was no public comment.

X. Adjournment

Lieutenant Governor Nuñez made closing remarks. The meeting was adjourned at 3:45 p.m.
State Governments at Risk: Cybersecurity Update

Florida Cybersecurity Task Force

December 3, 2019

Doug Robinson, NASCIO Executive Director
@NASCIO
About NASCIO

- National association representing state chief information officers and information technology executives from the states, territories and D.C.

- NASCIO's mission is to foster government excellence through quality business practices, information management, and technology policy.

- NASCIO provides members with products and services designed to support the challenging role of the state CIO, stimulate the exchange of information, and promote the adoption of IT best practices and innovations.
State Governments at Risk!

States are attractive targets – constant attack

More aggressive threats, more intensity

Nation state threats, organized crime

Critical infrastructure impact: disruption

Human factor – employees, contractors

Data and services on the move: cloud and mobile

Elections security
What’s the Current Situation?

▪ Critical life, health and safety systems must be available
  ▪ Public Safety
  ▪ Crucial services to citizens
▪ States hold billions of confidential records
  ▪ Personally Identifiable Information (PII)
  ▪ Personal Health Information (PHI)
  ▪ Intelligence
  ▪ Other confidential data
▪ Information integrity must be maintained
▪ Must be able to withstand and recover
### By the Numbers: Government Risk

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>75%</td>
<td>Hacks perpetrated by external actors in the government sector</td>
</tr>
<tr>
<td>94%</td>
<td>Email is the primary point of entry</td>
</tr>
<tr>
<td>2.5X</td>
<td>Public breaches are more likely to go undiscovered for years</td>
</tr>
<tr>
<td>#1</td>
<td>Government holds the top spot for both incidents and breaches</td>
</tr>
</tbody>
</table>
Cybersecurity involves more than just IT – it’s a business risk.

Protecting data and infrastructure is a core responsibility of state government entities and an investment in risk management.

It’s a complex ecosystem that requires governance and regular communication on risk.
STATE CIO TOP 10 PRIORITIES
2019 Strategies, Management & Process Solutions

1. Security and Risk Management
2. Cloud Services
3. Consolidation/Optimization
4. Digital Government
5. Broadband/Wireless Connectivity
6. Budget, Cost Control, Fiscal Management
7. Customer Relationship Management
8. Data Management and Analytics
9. Enterprise IT Governance
10. Identity and Access Management

Source: NASCIO State CIO Ballot, November 2018
Timeline of the Deloitte – NASCIO Cybersecurity Study

2010

A call to secure citizen data and inspire trust

2012

A call for collaboration and compliance

2014

Time to move forward

2016

Turning strategy and awareness into progress

2018

Bold plays for change
Ransomware, social engineering, and phishing are the top cyber threats for states

Please choose the prevalence of the following cyber threats in your state for the next year. (49 respondents)

<table>
<thead>
<tr>
<th></th>
<th>2018</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average threat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ransomware</td>
<td>35%</td>
<td>33%</td>
</tr>
<tr>
<td>Social engineering</td>
<td>32%</td>
<td>27%</td>
</tr>
<tr>
<td>Phishing, pharming, and other related variants</td>
<td>27%</td>
<td>18%</td>
</tr>
<tr>
<td>Somewhat higher threat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ransomware</td>
<td>43%</td>
<td>43%</td>
</tr>
<tr>
<td>Social engineering</td>
<td>41%</td>
<td>31%</td>
</tr>
<tr>
<td>Phishing, pharming, and other related variants</td>
<td>39%</td>
<td>35%</td>
</tr>
<tr>
<td>Very high threat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ransomware</td>
<td>16%</td>
<td>29%</td>
</tr>
<tr>
<td>Social engineering</td>
<td>27%</td>
<td>42%</td>
</tr>
<tr>
<td>Phishing, pharming, and other related variants</td>
<td>35%</td>
<td>47%</td>
</tr>
</tbody>
</table>

Source: 2018 Deloitte-NASCIO Cybersecurity Study
Survey question: Identify the top barriers that your state faces in addressing cybersecurity challenges.

Persistent challenges remain...

Budget, talent, and threats top three since 2010

2010  2012  2014  2016  2018

1.
Lack of sufficient funding

2.
Inadequate cybersecurity staffing

3.
Increasing sophistication of threats

Source: 2018 Deloitte-NASCIo Cybersecurity Study
Percent of IT Budget Spent on Cyber Averages 1 – 3%

Source: 2018 Deloitte-NASCIO Cybersecurity Study
51% Percent of States Had No Growth in Cyber Spending

Source: 2018 Deloitte-NASCIO Cybersecurity Study
48% Percent of States Have No Dedicated Cyber Budget

Source: 2018 Deloitte-NASCIO Cybersecurity Study
Talent Crisis in State Government

Top barriers to hiring, developing and retaining cyber talent

94% State’s salary rates and paygrade structures
51% Workforce leaving for private sector careers
47% Lack of qualified candidates due to demand from federal agencies and private sector
24% Work location—lack of qualified cyber workforce in the state capital
18% Outdated classifications and job descriptions for cybersecurity positions
12% Lack of a defined career path and opportunities in cybersecurity
12% Lengthy hiring process

Survey question: What are the top three human resource factors that negatively impact your ability to develop, support, and maintain the cybersecurity workforce within your state? (49 respondents)

Source: 2018 Deloitte-NASCIo Cybersecurity Study
61% of State CISOs Say That They Lack the Collective Competency to Manage Cyber Risks

Source: 2018 Deloitte-NASCIO Cybersecurity Study
Three Bold Plays for Change

1. ADVOCATE FOR DEDICATED CYBER PROGRAM FUNDING
   CISOs should raise cybersecurity’s visibility with the state legislature and executive branch by making it a line item in the IT budget. They can also seek funding from federal agencies to support compliance with those agencies’ security mandates.

2. CISOs AS AN ENABLER OF INNOVATION, NOT A BARRIER
   CISOs should actively participate in shaping the state’s innovation agenda, collaborate with state digital and innovation officers, and lead the charge to help program leaders securely adopt new technologies.

3. TEAM WITH THE PRIVATE SECTOR AND HIGHER EDUCATION
   CISOs should leverage public-private partnerships and collaborations with local colleges and universities to provide a pipeline of new talent, as well as consider outsourcing to private-sector firms.
The Responsive State CIO: Connecting to the Customer

2019 State CIO Survey
Please characterize the current status of the cybersecurity program and environment in state government.

<table>
<thead>
<tr>
<th></th>
<th>2019</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developed security awareness training for workers and contractors</td>
<td>92%</td>
<td>98%</td>
</tr>
<tr>
<td>Adopted a cybersecurity framework, based on national standards and guidelines</td>
<td>90%</td>
<td>94%</td>
</tr>
<tr>
<td>Acquired and implemented continuous vulnerability monitoring capabilities</td>
<td>86%</td>
<td>81%</td>
</tr>
<tr>
<td>Created a culture of information security in your state government</td>
<td>80%</td>
<td>79%</td>
</tr>
<tr>
<td>Established trusted partnerships for information sharing and response</td>
<td>82%</td>
<td>92%</td>
</tr>
<tr>
<td>Adopted a cybersecurity strategic plan</td>
<td>74%</td>
<td>85%</td>
</tr>
<tr>
<td>Developed a cybersecurity disruption response plan</td>
<td>61%</td>
<td>69%</td>
</tr>
<tr>
<td>Documented the effectiveness of your cybersecurity program with metrics and testing</td>
<td>55%</td>
<td>63%</td>
</tr>
<tr>
<td>Used analytical tools, AI, machine learning, etc. to manage cybersecurity program</td>
<td>49%</td>
<td>44%</td>
</tr>
<tr>
<td>Obtained cybersecurity insurance</td>
<td>47%</td>
<td>42%</td>
</tr>
</tbody>
</table>

What is the current role of your state CIO organization in administering the statewide cybersecurity program?

<table>
<thead>
<tr>
<th>Role</th>
<th>2019</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leading or participating in policy setting</td>
<td>92%</td>
<td>88%</td>
</tr>
<tr>
<td>Responsible for setting overall direction</td>
<td>92%</td>
<td>88%</td>
</tr>
<tr>
<td>Responsible for execution</td>
<td>80%</td>
<td>76%</td>
</tr>
<tr>
<td>Responsible for oversight</td>
<td>90%</td>
<td>86%</td>
</tr>
</tbody>
</table>
Whole-of-State Cybersecurity

Has your state adopted a whole-of-state approach to cybersecurity with collaboration among state agencies, local governments, utilities, private companies, universities, healthcare and others?

- 25% | Yes
- 22% | No
- 39% | In progress
- 14% | Planned
What Do We Know? Patterns of Success

- Enterprise Leadership and Governance
- Statewide Cybersecurity Framework & Controls
- Cybersecurity Culture: A Team Sport
- Know the Risks, Assess the Risks and Measure
- Communicating the Risks: Awareness
- Invest: SOC and Security Technologies
States Requiring .GOV Domain

Why? Critical for security
Why .gov?

Secure
HTTPS preloading ensures use of secure servers

Trusted
.gov is exclusive to U.S. government organizations

Authoritative
Oversight for the issuance of .gov domain names
Hot State Issues to Watch

- Elections security and disinformation
- Risk of emerging technologies – AI, IoT, UAS
- Third-party contractor security risks
- IT supply chain risks
- Public records laws/FOIA exemptions for cyber
NASCIO’s Cybersecurity Call to Action
Key Questions for State Leaders

- Does your state government support a “culture of information security” with a governance structure of state leadership and all key stakeholders?
- Has your state conducted a risk assessment? Is data classified by risk? Critical infrastructure reviewed? Are security metrics available?
- Has your state implemented an enterprise cybersecurity framework that includes policies, control objectives, practices, standards, and compliance? Is the NIST Cybersecurity Framework a foundation?
- Has your state invested in enterprise solutions that provide continuous cyber threat detection, mitigation and vulnerability management? Has the state deployed advanced cyber threat analytics?
- Have state employees and contractors been trained for their roles and responsibilities in protecting the state’s assets?
- Does your state have a cyber disruption response plan? A crisis communication plan focused on cybersecurity incidents?
CYBERSECURITY DISCUSSION WITH FLORIDA CYBER STATE TASK FORCE

December 3, 2019
Mike Housch is the Chief Information Security Officer for Black Knight. He is responsible for establishing and maintaining the enterprise information security vision, strategy, and program, ensuring information assets and technologies are adequately protected. Mike passionately leads global teams that drive operational security activities, vulnerability management, architecture, engineering, incident response, forensic operations, eDiscovery, litigation support, security governance, and regulatory audit oversight. Mike has a longstanding career serving in the CISO capacity of more than fifteen years and continues to drive change within Black Knight through innovation and effective management of the program.
Black Knight’s Sustainable Cybersecurity Management Program

**Effective security starts with the Tone from the Top,** ensuring support and compliance to security controls and processes.

**Employee Awareness**
- Define, implement, socialize security standards & controls
- Employee security awareness training and metrics
- Employee feedback when deviation detected

**Cohesive and Complete Logging, Monitoring, & Alerting**
- Comprehensive monitoring
- Identify & track misaligned applications, assets or processes
- Effective Data Loss Prevention (DLP) controls
- Incident Management: Develop playbooks & simulations to identify potential gaps

**Centralization (Public IP Space, Assets, Access and Logs)**
- Asset Management: Must have an exhaustive list and management process for all assets

**Centralized Access Management & Governance**
- User
- Privileged Access
- Third Party Access

**Effective Risk Governance**
- Phishing Management
- Security Metrics
- Policies and Standards
- Risk Reporting

**Strong Security Programs are well-designed, embracing all aspects of effective cybersecurity management**
- Security Operations Center
- Security Intelligence
- Threat & Vulnerability Management
- Security Testing
- Security Incident Management
- Security Architecture & Engineering
- Security Cloud Management
- Competitive Salaries
Black Knight’s Defense in Depth
Cybersecurity Management at Black Knight

**Threat & Vulnerability**
- Security Testing (Scans & Penetration Testing)
- Vulnerability Scanning (External & internal)
- Secure Code Management
- Security Controls Risk Assessments
- Security Intelligence
- DevSecOps

**Security Monitoring**
- Security Operations Center – SOC (7/24/365 active & centralized event monitoring)
- Threat Detection & Action (Data Leakage Prevention, Privileged User Monitoring, Malware Analysis, Intrusion Detection, Active Threat Hunting, Continuous Behavioral Monitoring for Abnormal Behavior)

**Security Architecture & Engineering**
- Security Architecture and Roadmaps
- Security Technology Support
- Security Cloud Architecture
- Security Engineering
Cybersecurity Management at Black Knight

**Security Incident Response**
- Centralized Security Incident Handling
- Forensics Security Investigations
- eDiscovery
- Litigation Support
- Tabletop Exercises

**Security Governance**
- Security Policies & Standards
- Security Reporting
- Security Oversight & Governance
- Security Exception Management
- Regulatory Agencies Liaison

**Security Cloud Management**
- Cloud Security Standards
- Cloud Secure Environments (AWS Landing Zone)
- Enforcement of Cloud Security Controls
- Active Cloud Event Monitoring
Cybersecurity Management at Black Knight

User Access
• Centralized User Access Lifecycle Management (Request, Approval, Fulfillment, Revalidations, Terminations/Transfers)
• User Access Certifications (On-going, Regular Validations of Lease-Privileged User Access)
• Mainframe Access Management (RACF)

Privileged Access
• Centralized Management of Privileged User Passwords (Check-in/check-out; automated password changes)
• Privileged Access Monitoring & Certifications
• Service Account Management (System-to-System Accounts)

Access Strategy & Applications
• Establish and Manage Strategy and Roadmap for Access Management (User, Privileged & System)
• Development, Testing & Deployment of Access Products/Applications
Cybersecurity Management at Black Knight

**Third-Party Risk Management**
- Centralized Management of the Third-Party Lifecycle Process (Initiation/RFP, Assessment, On-Boarding, Monitoring, Termination)
- Ongoing Monitoring of Third-Parties (Security, Financial, Reputation, Legal, Business, Country, etc.)

**Business Continuity**
- Centralized Continuity Management (Business Continuity, Disaster Recovery, Crisis Management)
- On-Going Testing and Updates (Table-Top & Real-Time Testing, Updating Plans, RPOs, RTOs, etc.)

**Risk Management**
- Establish and Manage Risk Policies, Standards, Strategies and Roadmaps.
- Manage Risk Identification, Risk Measurement, Risk Reporting & Risk Remediation
- Phishing Exercises
- Division Liaison

Confidential, Proprietary and/or Trade Secret | TM SM ® Trademark(s) of Black Knight IP Holding Company, LLC, or an affiliate. © 2019 Black Knight Financial Technology Solutions, LLC. All Rights Reserved.