ENTERPRISE CYBERSECURITY IS JOB SECURITY

A Guide to Protecting Your Global Mobility Program

Enterprise Cybersecurity Is Job Security

A GUIDE TO PROTECTING YOUR GLOBAL MOBILITY PROGRAM

Hacks, ransomware and data breaches make headlines daily. This should give pause to anyone whose business entails managing and securing confidential information. As an in-house mobility professional responsible for employee data, you should think about how to best identify and mitigate risk, protecting your company and its people.

If you run a mobility program, large or small, you need to make sure your employees' data is protected and your immigration provider's case-management software meets the highest security standards.

Choosing the right immigration provider is a must for your company and your personal success. But how do you select the right provider to protect your company's employees?

HERE ARE SOME KEY CONSIDERATIONS TO KEEP IN MIND AS YOU REVIEW PROVIDERS

- What security governance questions should be asked in the RFP process?
- What questions will help you determine if your immigration provider follows best security practices?
- Who in your organization should be involved in security decisions regarding employee data?
- How can internationally recognized security and privacy standards, such as ISO 27001, factor into your evaluation?
- What are provider mandatories when it comes to overall data protection and case management security?

Contents.

I. Governance

Approaches to Cybersecurity Governance

BASICS FOR RFP PREPARATION

When selecting an immigration provider, you will ask numerous questions about their program and service delivery. You will probably address systems security, but it's also important to review your potential providers' security strategies for technology and their operations overall. Often, the weakest links in an organization's data security are its people.

Best-in-class security operations should include a fully engaged executive management team. Such a team should offer dedicated personnel and programs. It should also provide a documented set of policies, procedures, guidelines, and standards that ensure the confidentiality, integrity, and availability of data through effective security management practices and controls.

A provider's information security governance program should include all of the necessary tools, personnel, and business processes required to actively manage security and data protection controls. An effective program must encompass all relevant controls across three security master categories:

- Logical/Technical
- Physical
- Administrative/Organizational

What types of information security protocols does the provider employ for comprehensive protection of your global mobility program? Hacks and ransomware are top of mind, but it's important to look at the big picture.

Governance is the foundation of all security matters. If strategic planning, strong leadership, and good documentation guide the overall security program, rest assured that your provider takes security seriously.

ASK THE POTENTIAL PROVIDER

- Does your firm have a dedicated security team?
- Who leads your security team?
- What form does your governance take?
- Are your top leaders invested in cybersecurity governance?
- What types of annual training do you require for employees?
- What are the key features of your security program's governance structure?
- What types of security protocols have been implemented, documented and validated?

Key Features of Security Governance

STRATEGIC PLANNING

AN IMMIGRATION PROVIDER'S SECURITY STRATEGY SHOULD ESTABLISH A COMPREHENSIVE GOVERNANCE FRAMEWORK FOR MONITORING AND IMPROVING THE OVERALL DATA PROTECTION PROGRAM.

ORGANIZATIONAL STRUCTURE

THE PROVIDER'S SECURITY PROGRAM SHOULD BE CENTRALIZED AND INCLUDE EXECUTIVE MANAGEMENT, ENSURING HOLISTIC, RISK-BASED GOVERNANCE THROUGHOUT THE ORGANIZATION.

SECURITY POLICY AND GUIDANCE

IMMIGRATION PROVIDERS SHOULD OFFER CLIENTS A SET OF CYBERSECURITY POLICIES, PROCESSES AND PROCEDURES THAT SUPPORT OVERALL GOVERNANCE ACROSS THE ENTERPRISE.

ESTABLISHMENT OF ROLES AND RESPONSIBILITIES

KEY GOVERNANCE POSITIONS (CIO, CSO, SECURITY PERSONNEL, ETC.) MUST BE IN PLACE. THE PROVIDER'S SECURITY RULES AND REGULATIONS SHOULD REQUIRE DEDICATED PERSONNEL SUPPORTING THE OVERALL PROGRAM.

SECURITY GOVERNANCE INTEGRATION WITHIN THE ENTERPRISE ARCHITECTURE

CONTROLS SHOULD BE BUILT INTO THE PROVIDER'S SYSTEMS, INFRASTRUCTURE AND APPLICATIONS ACROSS THEIR ARCHITECTURE TO ENSURE SECURITY AND DATA PROTECTION THROUGHOUT THE ENTERPRISE'S TECHNICAL ENVIRONMENT.

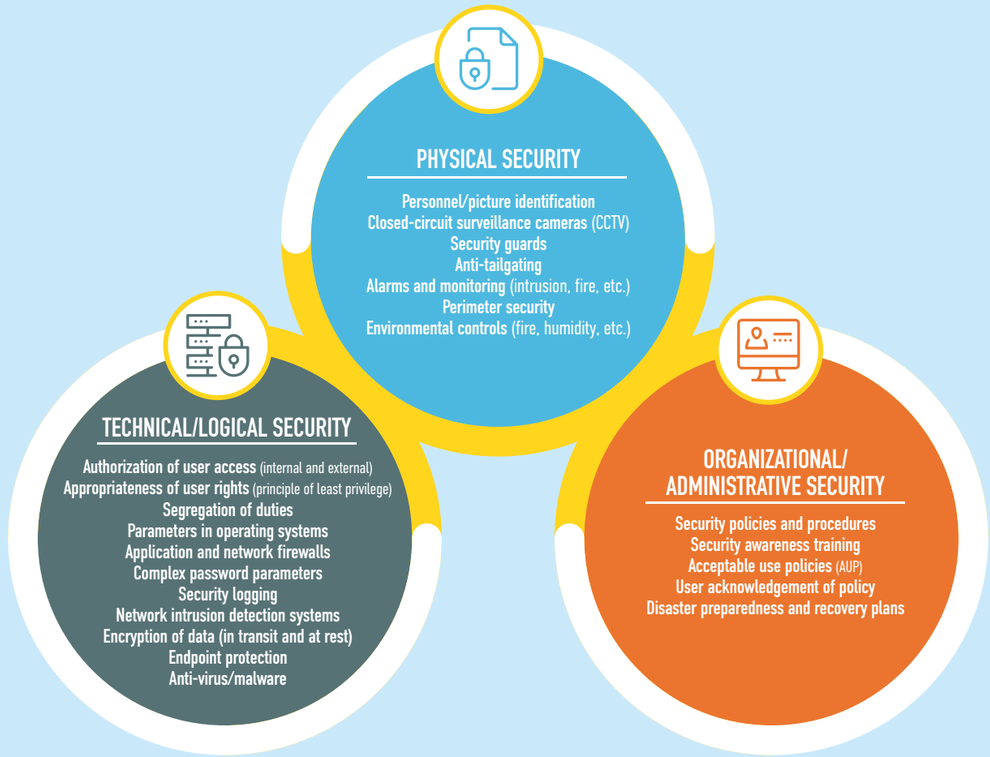
II.
Controls

Understanding Data Security Controls

Recently, big law firms and immigration providers have made headlines because of security breaches and ransomware attacks. The security of immigration case management software is a critical decision factor for many immigration teams.

Governance ensures that controls are put in place across different domains, including technical and logical, physical, and organizational areas. When assessing a provider, you will want to make sure their controls are comprehensive and well-thought-out in each of the three domains.

SOME KEY CONTROLS ACROSS DIFFERENT DOMAINS



TECHNICAL CONTROLS

Immigration providers' security programs focus on preventative, detective and corrective controls to manage technology risks such as data breaches. Complex, high-volume immigration relies on advanced technology platforms, and immigration information processing requires robust protection to ensure your peace of mind.

When selecting a provider, you should ask questions to understand what kind of controls they place on their systems. You may wish to engage your company's security and IT departments to put expert eyes on technical responses to topics like end-point detection, penetration testing, and encryption.

COMPONENT	PREVENTATIVE	DETECTIVE	CORRECTIVE
Forensics: Endpoint Threat Detection and Response		X	X
Cyber Intelligence Services	X		
Data Classification Enforcement	X		X
DLP (Data Loss Prevention)	X		X
Endpoint AV/Malware Protection	X	X	X
Endpoint Encryption	X		
File Integrity Management (FIM)	X		X
Firewall	X		
Identity Management	X		
IDS/IPS (Intrusion Detection/Prevention System)	X	X	
Incident Response		X	
MDM (Mobile Device Management)	X	X	
Multi-Factor Authentication	X		
Penetration Testing	X		
PKI (Public Key Infrastructure)	X		
Privileged Access Management	X	X	
SIEM (Security Incident and Event Monitoring)			
Single Sign-On	X		
VPNs (Virtual Private Networks)	X		
Vulnerability Scanning for Servers/OS	X	X	
Web Application Firewalls	X	X	
Web Application Scanning/Dynamic Code Scanning		X	
Web Proxies	X	X	

LOGICAL SECURITY

Limiting access to information on a "need to know" basis is an important cybersecurity measure. Ask your immigration provider how their systems and organizational policies address user access. Logical access for systems should be governed by strict security policies with differing requirements for users with elevated privileges. Access should be approved, periodically reviewed for appropriateness, and removed when there is no longer a business need.

PHYSICAL SECURITY

Physical security is often one of the weakest aspects of a security program. Don't overlook how your immigration provider secures assets and locations. Best practice requires a physical office that is secured 24/7, with an access-control system and tangible barriers.

Visitors should present a valid photo ID for approval to enter. They should wear temporary badges and be escorted at all times. Badges should offer limited access within the building and be valid only for the date of issuance.

Operations and security teams should monitor and enforce environmental sensors, alarms and other physical notifications. All security and environmental systems should be supported by redundant power, uninterruptible power supply (UPS) devices, and stand-by generators.

Your immigration provider should have a clear desk/clear screen policy, as well as policies and protocols for safekeeping physical documents, such as passports and other sensitive materials. Policies should ensure sensitive documents or other employee data are stored securely and disposed of properly.

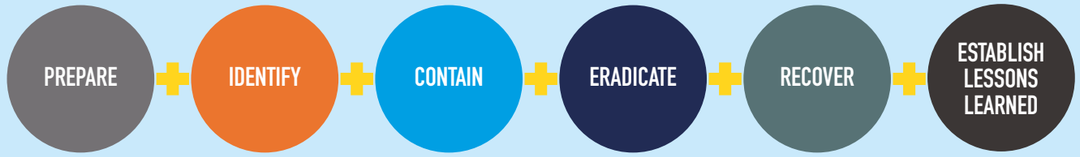
SECURITY TRAINING

Immigration providers should have training programs in place to keep employees and contractors updated on security practices. Relevant personnel should complete security and privacy awareness training that includes:

- Confidentiality
- Integrity
- Availability
- Accountability
- How these apply in the workplace

DATA SECURITY INCIDENT RESPONSE

Your provider should have an established, comprehensive security incident response plan, with processes and procedures designed to:



The response plan should be initiated in the event of unauthorized access, disclosure, theft, misuse, alteration, or destruction of any protected data on the provider's systems or network.

ASK THE POTENTIAL PROVIDER

- What physical security policies are in place?
- What is your data security incident response plan?
- How are your employees trained and how often?
- Who has access to information in your system and how often is system access reviewed?

III. Frameworks

The Value of Cybersecurity Frameworks

INTERNATIONAL STANDARDS AND THIRD-PARTY CERTIFICATIONS

Assessment of a new provider's immigration case-management system usually occurs during the RFP process and onboarding. Often, global mobility team leads will be tasked with evaluating software security, and it's important for in-house mobility teams to know best-practice standards. At a minimum, teams should be familiar with third-party certifications for providers and their technology offerings, such as ISO 27001.

WHAT IS ISO 27001?

The ISO/IEC 27001 standard is a framework published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This internationally recognized standard defines the requirements for implementing and maintaining an Information Security Management System (ISMS). It helps organizations manage their information security program centrally and consistently.

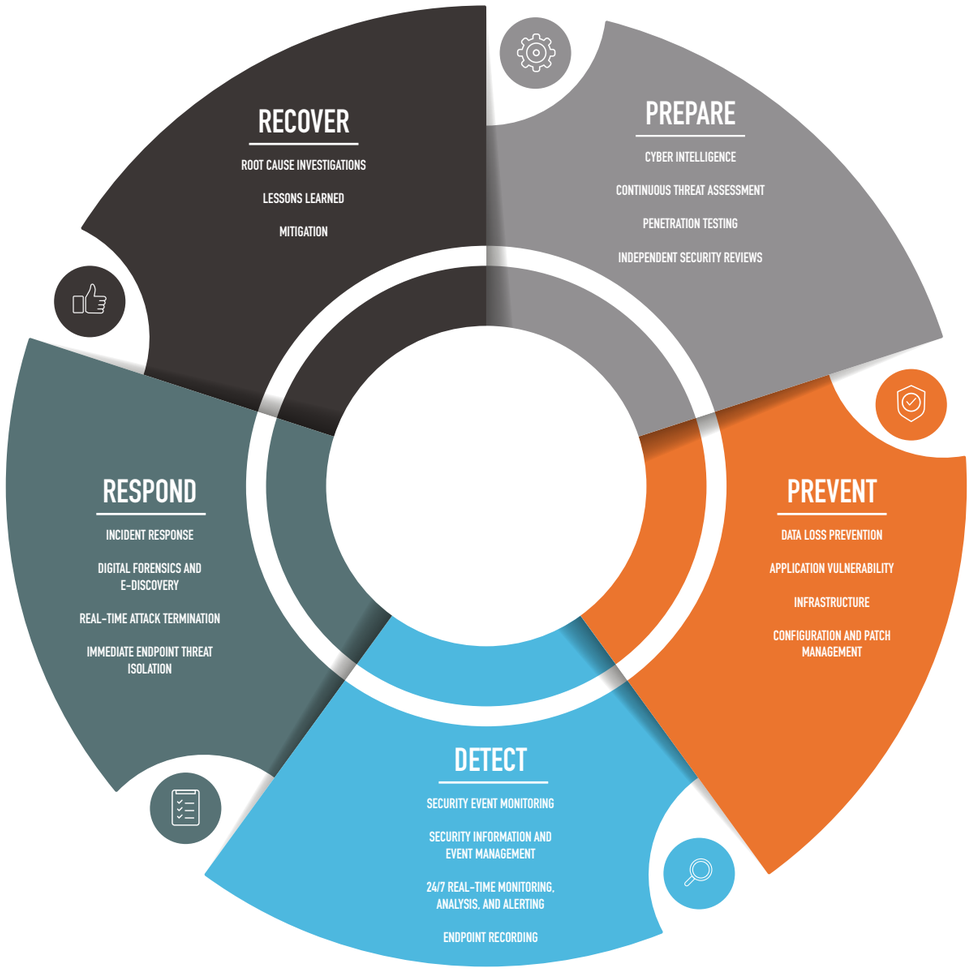
Data security threats exploit the increased complexity and connectivity of critical systems. The establishment of an ISMS, in accordance with the ISO 27001 standard, ensures immigration providers apply a risk-based approach to protecting the data they're entrusted with, ensuring the confidentiality, integrity, and availability of their clients' information.

Providers can exhibit adherance to the ISO 27001 standard with the implementation of five concurrent and continuous information security functions:

- Prepare
- Prevent
- Detect
- Respond
- Recover

Together, these functions support the life cycle of an organization's information security management program.

INFORMATION SECURITY UNDER THE ISO 27001 FRAMEWORK



ASK THE POTENTIAL PROVIDER:

- What security framework does your organization use to guide your data protection programs?
- What type of third-party security audit do you perform and on what schedule?

IV. Conclusion

Data Security Must-Haves

When you select an immigration provider, avoid making a decision in a vacuum; security is too important and the consequences are too high. Whenever possible, engage other stakeholders to help you assess providers and apply due diligence in all areas. Involve Security, IT, Privacy, and Procurement for insights in areas where you might lack expertise.

RFP questions for an immigration program provider generally focus on program management and may not directly address employee data security protocols. Remember that a truly secure immigration program must be designed into a provider's foundation, and governance is key to a strong, reliable program.

The best security programs cannot be reverse engineered by applying Band-Aids like extra penetration testing or end-point software testing. Effective programs should address every aspect of security across the three domains of controls: technical/logical, physical, and administrative/organizational.

If you have additional questions about immigration program security, please reach out to cybersecurity@balglobal.com to schedule a consultation.

V. Question Bank

Sample RFP Security Questions

We've put together a list of RFP questions that will help you dig deeper into the most important aspects of security, ensuring that your provider offers a solid, serious, and sophisticated approach to security governance.

GENERAL SECURITY GOVERNANCE

- Who leads your security team? Describe your experience with leading security programs.
- Do you have defined executive support and management oversight of the security program?
- What types of security protocols has your organization documented?
- What are your security policies? Describe the general application of your security policies enterprise-wide.
- What is your high-level, enterprise-wide security strategy?
- Do you use third parties to access employee-immigration data? If so, what are your management controls?
- Do you perform regular internal audits of your policies, processes, and security control environment?
- Are you audited by a third party on a consistent basis? What independent certifications do you maintain?

TECHNICAL AND LOGICAL CONTROLS

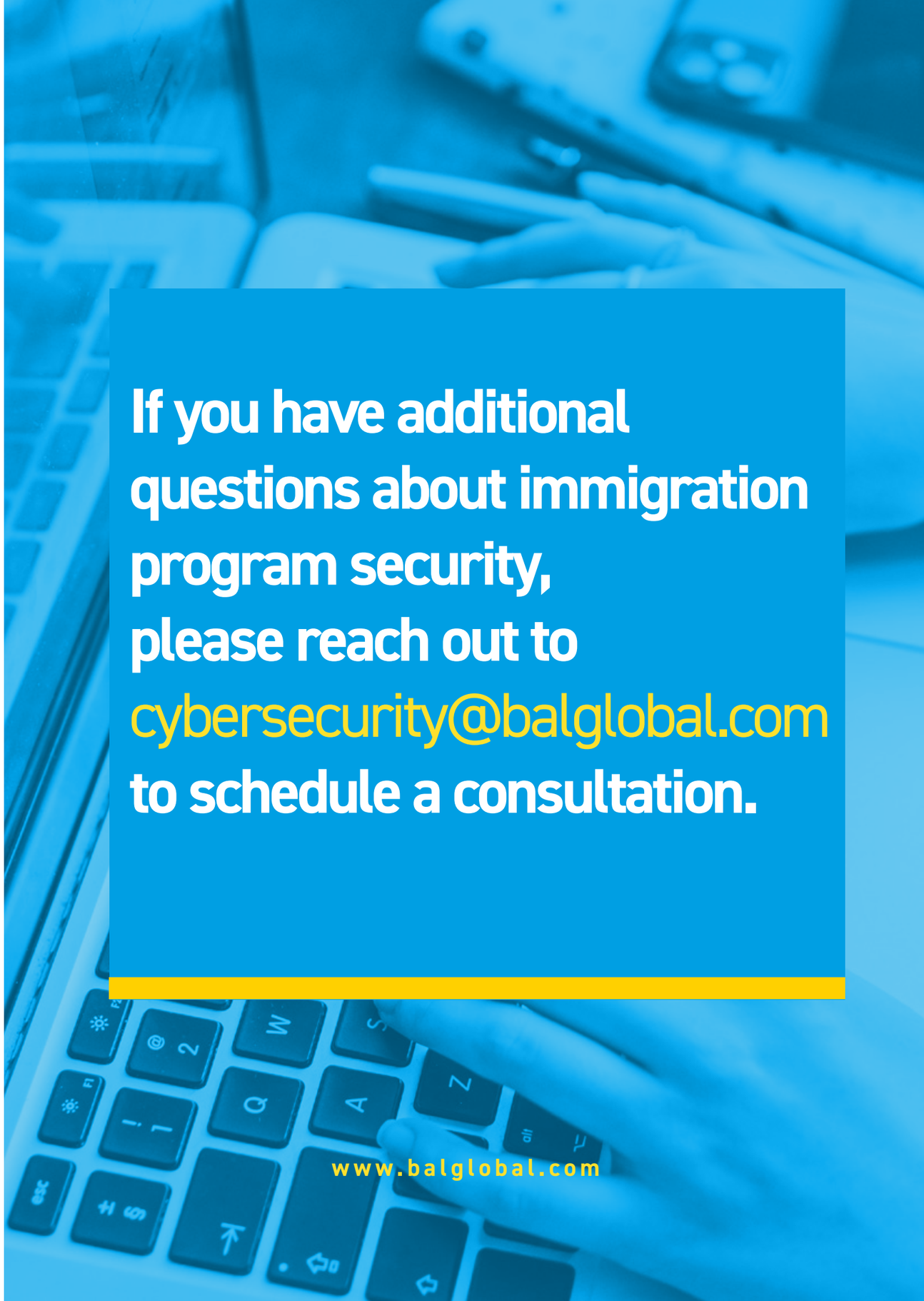
- What type of access logs do you maintain and for how long? If an incident occurs, how will you trace the transaction in the logs? How are logs managed, and for how long are they retained?
- What are your methods for managing application secrets, including encryption keys and backend services credentials?
- Does your system provide tokens as secondary authentication for read-and-signs or electronic signatures for certificates?
- Do you have a proper, effective, logical separation between Dev/Quality (Testing) and Production environments?
- Do you have an industry-best-practice password policy? What are your policies for changing and sharing passwords? How are passwords stored?
- What is your access control policy?
- Do you perform external penetration tests at least quarterly and internal network security audits at least annually?

TECHNICAL AND LOGICAL CONTROLS CON'T.

- What is your policy on patching?
- What is your backup policy? Is there a Disaster Recovery Plan to protect immigration data? What are your recovery time objectives and recovery point objectives (RTO/RPO)?
- Is your case-management software and equipment tested under full-load conditions? What types of load testing have your systems been subjected to?
- Does your system provide a single administrative portal for the management of role-based account actions?
- Who are your authorized users that decrypt or view data in unencrypted form, including system administrators, database administrators, or others? What controls exists around this access?
- Do you have protections against the Open Web Application Security Protection (OWASP) Top 10 (i.e. XSS prevention, CSRF protection, etc.)?
- Can you present a documented set of controls for ensuring the separation of data and the security of information between different customers' SaaS instances?
- Do you have a set of controls to ensure information is not mistakenly disclosed to unauthorized persons?
- Do your hosting environments provide redundancy and load balancing for firewalls, intrusion prevention, and other critical security elements?
- Do you have controls to address the threat of information knowingly being misused by your workforce and contractors, including background checks, role-based access to information, and other relevant safeguards?
- What mechanisms do you use to transport data? What methods are used to safeguard data during transport?
- What types of APIs can access your systems, including custom and user-defined fields?

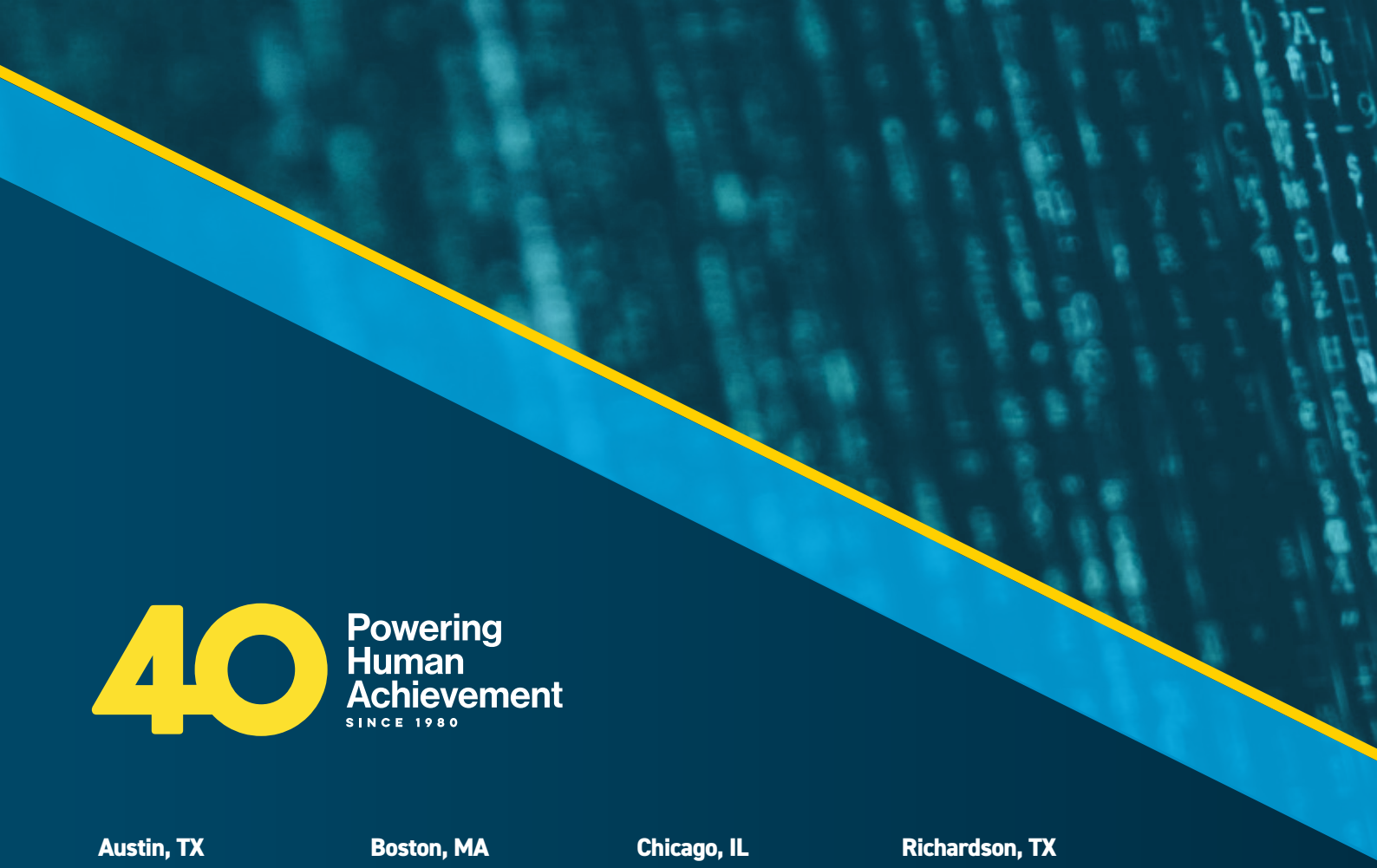
PHYSICAL AND ADMINISTRATIVE CONTROLS

- How do you secure your physical premises?
- Do you use electronic key cards?
- Do you use a hosted or cloud-based data center? If so, are independent audit reports obtained, reviewed and approved on a regular basis?
- Do you have a clear desk/screen policy?
- What policies do you have regarding physical documents, printer usage, and disposal of printed documents?
- How do you store documents? Describe your data retention and disposal processes.
- What type of security training is required of your employees and contractors? How often?
- Describe controls you use to address the threat of physical theft or loss of data.
- Describe your security-incident response procedures for a physical breach or breach caused by human error.
- What are your policies or sanctions for employees who cause a security breach?



If you have additional questions about immigration program security, please reach out to cybersecurity@balglobal.com to schedule a consultation.

www.balglobal.com



40 Powering Human Achievement
SINCE 1980

Austin, TX
700 Lavaca Street
Suite 1400
Austin, TX 78701
Tel +1 737 252 5400
Fax +1 512 334 6001

Boston, MA
265 Franklin Street
Suite 502
Boston, MA 02110
Tel +1 857 309 5100
Fax +1 617 482 0975

Chicago, IL
1 S Wacker Drive
Suite 1630
Chicago, IL 60606
Tel +1 312 682 9704
Fax +1 312 275 7565

Richardson, TX
2400 N Glenville Drive
Building A
Richardson, TX 75082
Tel +1 469 654 3200
Fax +1 469 729 5886

Houston, TX
10100 Katy Freeway
Suite 600
Houston, TX 77043
Tel +1 346 278 6500
Fax +1 832 871 4004

McLean, VA
8300 Greensboro Drive
Suite 550
McLean, VA 22102
Tel +1 571 412 4100
Fax +1 571 316 2356

New York, NY
11 Times Square
11th Floor
New York, NY 10036
Tel +1 929 335 9800
Fax +1 646-981-2099

San Francisco, CA
50 California Street,
2nd Floor
San Francisco, CA 94111
Tel +1 628 215 2800
Fax +1 415-398-1808

Santa Clara, CA
4555 Great America Pkwy,
Suite 210
Santa Clara, CA 95054
Tel +1 650 419-9100
Fax +1 408-762-4756

Walnut Creek, CA
100 Pringle Ave
Suite 300
Walnut Creek, CA 94596
Tel +1 925 278 5100
Fax +1 925-378-6250

Washington, D.C.
1133 Connecticut Ave. NW
Suite 1050
Washington, D.C. 20036
Tel +1 571 536 6700
Fax +1 202 688 3744

B · A · L

www.balglobal.com