**IT Cyber System Overview**

The ALTA Information Security Work Group has developed this overview and the companion workbook to help title agents conduct a complete inventory of their IT Cyber Systems including hardware, software, and services. This inventory is an essential step to begin guarding against cybersecurity incidents and to prepare to react quickly and effectively should a cybersecurity incident occur. The inventory, along with regular reviews and updates, will prepare a title agency to quickly recognize any components which may need to be upgraded, repaired, replaced, or further secured.

This **IT Cyber System Overview** is referenced in the ALTA **Cybersecurity Incident Response Plan Template**. Both documents are available on the ALTA website’s Information Security page at <https://www.alta.org/business-tools/information-security.cfm>.

**Hardware Inventory**

A Hardware Inventory should include any equipment or device which is attached to your computer network either physically with a cable, wirelessly via WiFi connection, through mobile application, or by remote connection over the Internet.

Here are some examples of what to look for during your Hardware Inventory:

* IT Networking Equipment
	+ Firewall, Router, Switch, Wireless Access Points
* Computer Hardware
	+ Servers
	+ Desktops/Laptops
* Peripherals
	+ Copiers, Printers, Scanners
* Security Devices, Appliances, or Services
	+ Intrusion Detection System (IDS), Intrusion Protection System (IPS)
	+ Email Filtering, SPAM Filtering
* Mobile Devices
	+ Smart Phones, Tablets
* Internet of Things (IoT)
	+ Security Systems
	+ Smart Cameras; Smart Door Locks
	+ Climate Control Systems
	+ Google Home; Amazon Alexa
* Remote & Work From Home (WFH) Workers
	+ Remote worker preferences – anything goes? Are they using company hardware? Personal hardware?

**Software & Services Inventory**

Your company likely owns and has licenses to use many, many types of software products. You’ll have general business software like Microsoft Outlook, Word, and Excel; accounting or payroll software; title production software; access to bank systems software online; access to online calendaring systems.

When you conduct a software inventory, be sure to consider where software resides (e.g., locally in your office environment, online but stored in your own data center, web-based, in the cloud as provided by a vendor). You should also consider all of the connected applications attached to your software (e.g., plug-ins or add-ins to the software interface), other software integrations (e.g., API), and Software-as-a-Service (“SaaS”).

Also during the inventory, consider which software components are essential to your operation. Can you be without email for a day or a week? Can you operate without it for any length of time? Learn more about how to assess the essential nature of software components in the **Business Impact Analysis Overview**, also available on ALTA website’s Information Security page at <https://www.alta.org/business-tools/information-security.cfm>.

Here are some examples of what to look for during your Software & Services Inventory:

**General Business Software**

* Word Processing; Spreadsheets; Presentation
* Communications Local or Cloud (e.g., email, fax, text/chat, calendaring/scheduling, add-ins/plug-ins to other software products)
* Contact Management
* Human Resources (e.g., payroll, benefits, background checks)
* Security Software Systems (e.g., email/SPAM filtering)

**Industry-specific Software**

* Title Production
	+ Title Production Software
* Closing & Settlement
	+ eSignature; Remote Online Notary (RON)
* Payments
	+ Escrow Accounting Software; Bank Reconciliation Software; Online Payment Systems

**Services**

* Data Center Hosting
* Website(s), Portal(s), and Website Hosting
* Domain Name Registration and Domain Name Services (DNS) Hosting (i.e., my agency.com)
* Multi-factor Authentication (MFA)
* Managed Service Provider (MSP)
* Internet Service Provider (ISP)
* Document Sharing Services (e.g., Dropbox, iCloud, GoogleDocs)
* Monitoring Tools (e.g., network monitoring, vulnerability scanning, cyber risk assessment)

See accompanying **Cyber System Hardware and Vendor Inventory Workbook** available on the ALTA website’s Information Security page at <https://www.alta.org/business-tools/information-security.cfm>