Dr. Theodoros Ntouskas

Security Compliance Trends

11th Infocom Security Conference: 22.04.2021

ict PROTECT
INFORMATION SECURITY SERVICES

www.ictprotect.com

Security Compliance Trends - Topics

ict PROTECT
INFORMATION SECURITY SERVICES

- **Introduction**
- **Last year events & changes**
- **COVID 19 “effect” in Cybersecurity**
- **Compliance Trends for Cloud Services**

Information Security: Is it a New requirement?

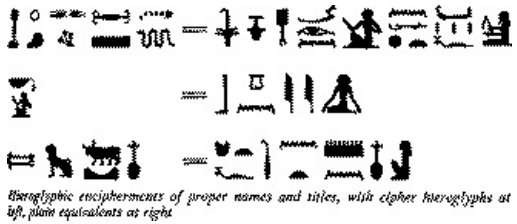
ict PROTECT
INFORMATION SECURITY SERVICES

- ✓Ancient Egyptians : encryption of hieroglyphics in monuments.
- ✓Ancient Greeks: “Κρυπτεία σκυτάλη”
- ✓Maya writing system
- ✓Caesar Cipher
- ✓Enigma

Confidentiality

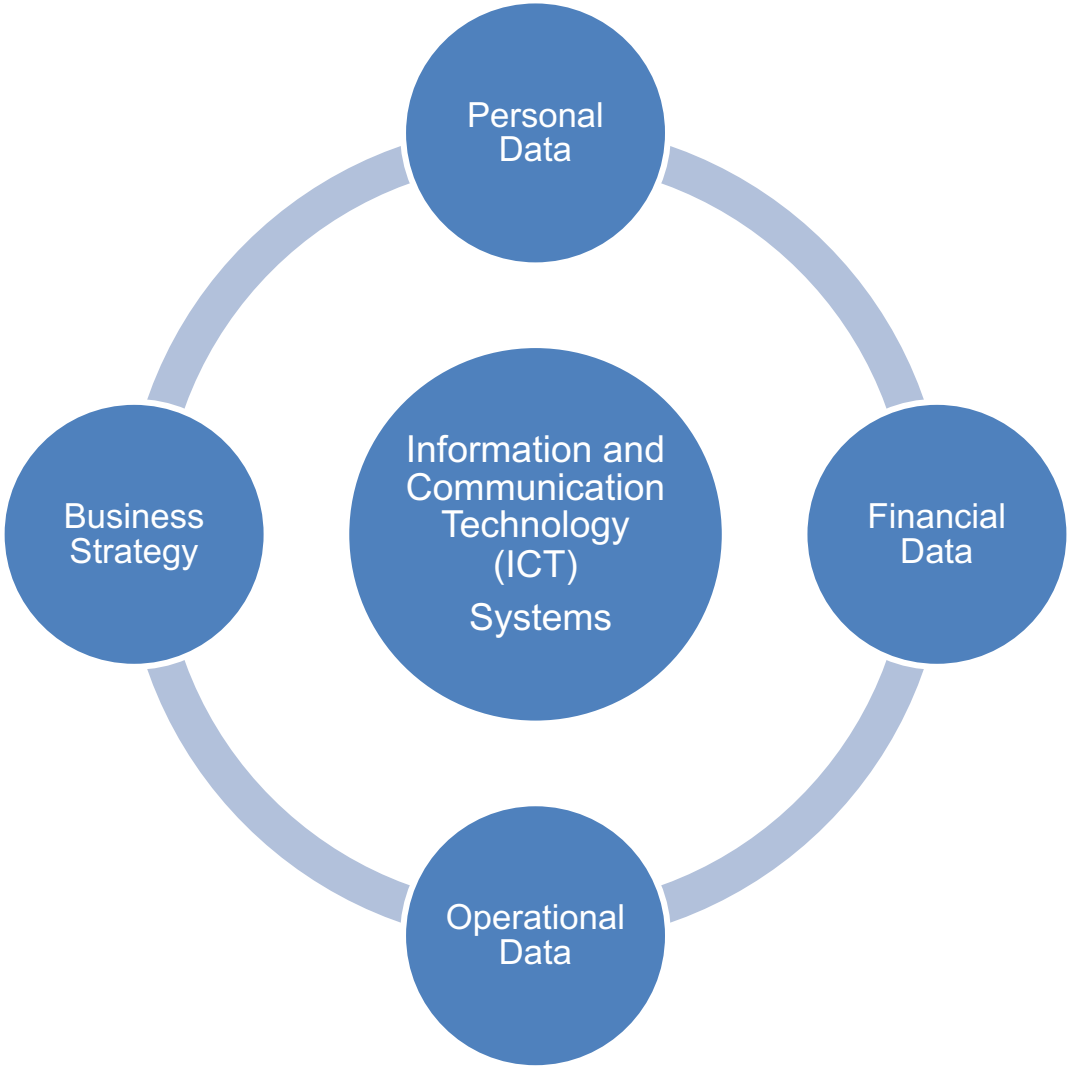
Integrity

Availability



Hieroglyphic encipherments of proper names and titles, with cipher hieroglyphs at left, plain equivalents at right

Introduction



Last year events … & changes

ict PROTECT
INFORMATION SECURITY SERVICES

COVID-19 Pandemic Event

- Lockdowns have permanently changed everything about how we conduct business.
- New Virtual shops due to lockdown
- Remote work: the new workspace reality
- The adoption of Cloud Services has been increased
- Find the cheapest and not the most secure solution

Issues from Data Transfer

- Brexit & UK GDPR
- Privacy Shield: *Schrems II* decision

Issues from Third parties

- Unavailability of Data Centers (e.g. fire event - early March 2021)
- Security Breaches have been increased: e.g
  - Solarwinds case impacted > 18.000 customers
  - Attacks at medical institutes (i.e. a hospital in Germany was locked out of their systems and unable to treat patients)
- to be continued ...

Other

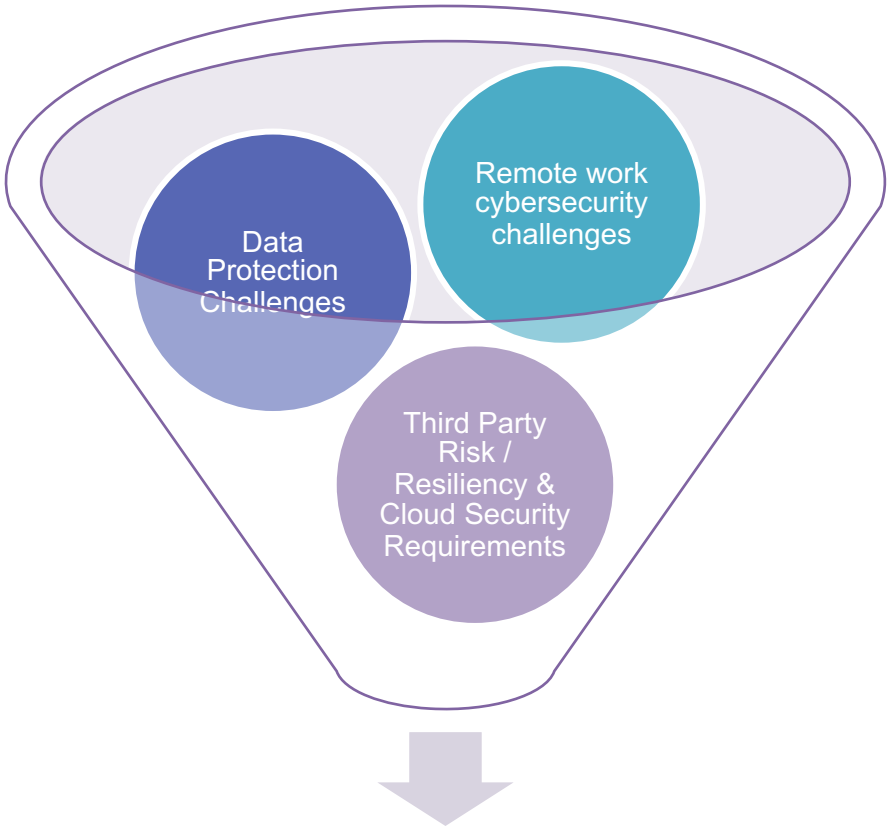
- IMO 2021 - MSC.428 :Maritime Cyber Risk Management
- The European Commission proposed a Digital Operational Resilience Act (DORA)

GDPR

UK GDPR

CCPA

HIPAA



New Information Security Compliance "arena"

ISO 22301

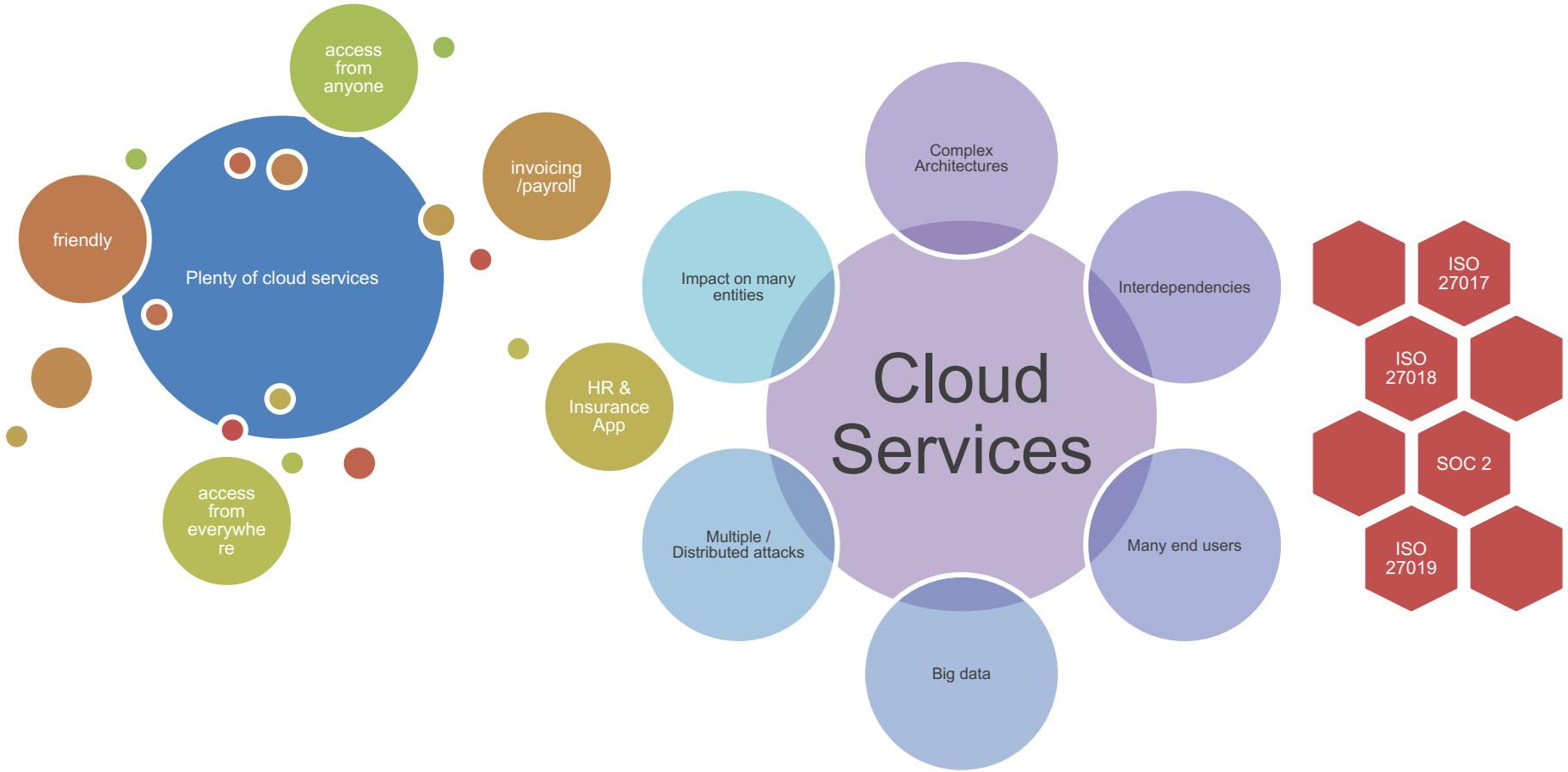
ISO 27701

ISO 27017

ISO 27018

SOC 2 (AICPA TSC)

Third Party Risk / Resiliency & Cloud Security Requirements



ISO/IEC 27017 Main Info

- **ISO/IEC 27017** is a code of practice for information security controls based on **ISO/IEC 27002** developed for **cloud services**.
- The standard advises both **Cloud Service Customers** and **Cloud Service Providers**.
- Provides additional cloud-specific implementation guidance based on **ISO/IEC 27002** controls.
- Provides additional controls to address cloud-specific information security threats and risks considerations.

ISO/IEC 27017 Main Requirements

The standard provides cloud-based guidance on 37 of the controls in ISO/IEC 27002 but also features seven new cloud controls that address the following:

I. **Shared roles and responsibilities within a cloud computing environment**
II. **Removal of cloud service customer assets**
III. **Segregation in virtual computing environments**
IV. **Virtual machine hardening**
V. **Administrator's operational security**
VI. **Monitoring of cloud services**
VII. **Alignment of security management for virtual and physical networks**

ISO/IEC 27018 Main Info

- **ISO/IEC 27018** is the first international code of practice for **cloud privacy.**
- It helps **Cloud Service Providers** who process **Personal Identifiable Information (PII)** to assess risk and implement controls for protecting PII.
- Specifies guidelines based on **ISO/IEC 27002**, taking into consideration the regulatory requirements for the **protection of PII**.
- Adds PII to the scope of **ISO/IEC 27001** and emphasizes in additional controls that must be implemented in order to **increase the level of protection of personal data in cloud services.**
- Applicable to **all types and sizes of organizations**, including public and private companies, government entities and not-for-profit organizations, which provide information processing services as **PII processors via cloud computing** under contract to other organizations.
- Can also be relevant to organizations acting as **PII controllers**.
- ISO Certification is endorsed.

Cloud Security Requirements
ISO/IEC 27018 Main Requirements

ict PROTECT
INFORMATION SECURITY SERVICES

- Obligation to co-operate regarding PII principals' rights
- Public cloud PII processor's purpose
- Public cloud PII processor's commercial use
- Secure erasure of temporary files
- PII disclosure notification
- Recording of PII disclosures
- Disclosure of sub-contracted PII processing
- Notification of a data breach involving PII
- PII return, transfer and disposal
- Restriction of the creation of hardcopy material
- Control and logging of data restoration
- Protecting data on storage media leaving the premises
- Use of unencrypted portable storage media and devices
- Encryption of PII transmitted over public data-transmission networks
- Secure disposal of hardcopy materials
- Unique use of user IDs
- User ID management
- Contract measures
- Sub-contracted PII processing
- Access to data on pre-used data storage space
- Geographical location of PII
- Intended destination of PII

SOC: *Service Organization Controls*

SOC is an information security compliance standard created by the American Institute of Certified Public Accountants (AICPA)

Types of SOC reports:

- **SOC 1** is focused on the effectiveness of internal controls related to financial controls in order to protect customer data.
- **SOC 2** is focused on Information and IT Security identified by any of the five AICPA Trust Services Criteria related to *Security*, *Availability*, *Processing Integrity*, *Confidentiality* and *Privacy*.
- **SOC 3** covers the same procedures as a SOC 2 report, but it is intended for general public distribution without the detailed test results of SOC 2.

Type of audit reports

- Type I validates the design of controls
- Type II reviews / audits Service Organization's controls over a specific period of time (6 to 12 months) and ensures that controls are properly designed and operating effectively.

Security Management: A world of …requirements!

ict PROTECT
INFORMATION SECURITY SERVICES

GDPR

ISO 22301

IMO

UK GDPR

ISO 27701

NERC CIP

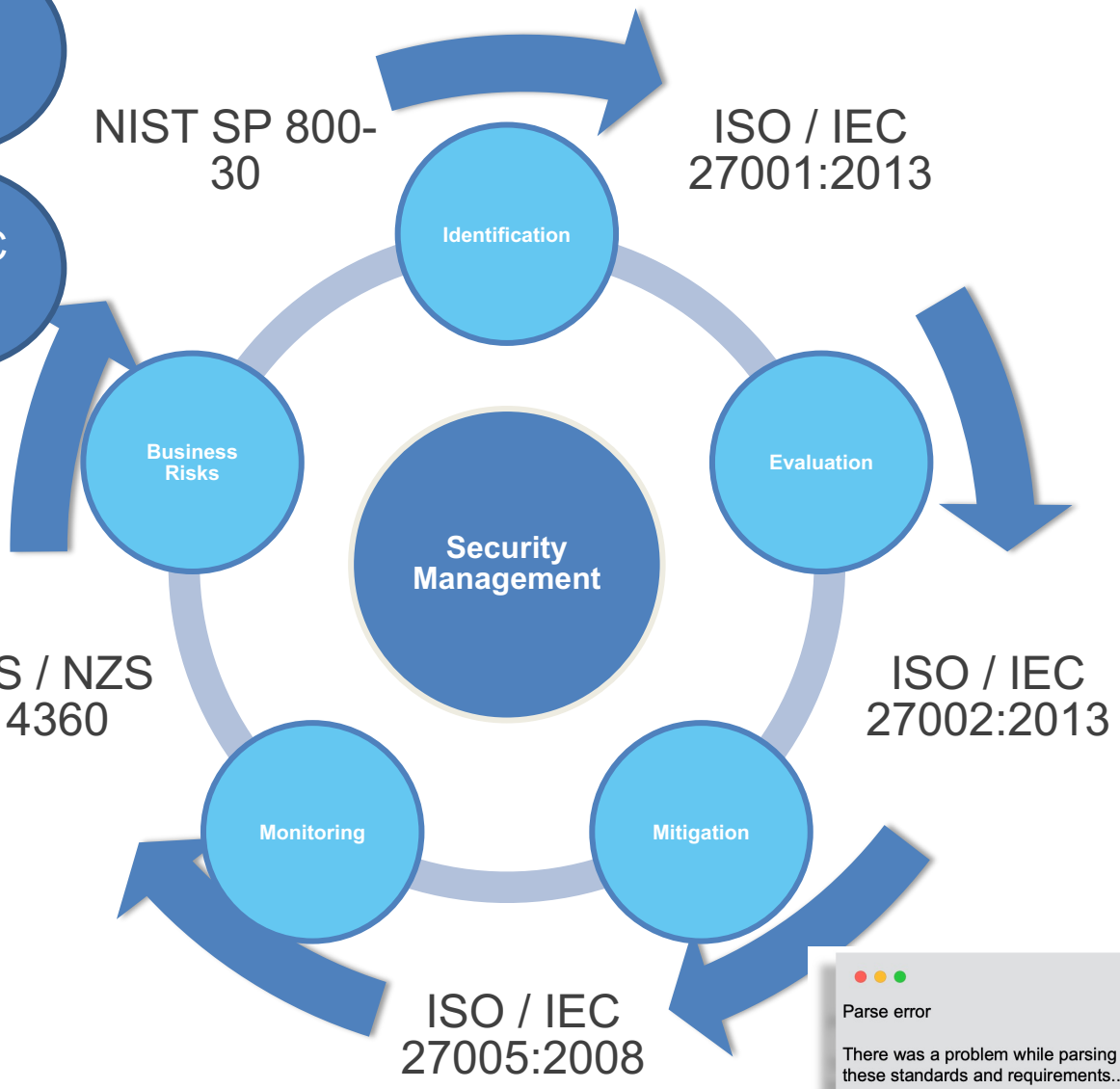
CCPA

ISO 27017

HIPAA

ISO 27018

SOC 2 (AICPA TSC)



Parse error

There was a problem while parsing all these standards and requirements..

ICT PROTECT Compliance Methodology

Cancel

Our Proposed Compliance Methodology

ict PROTECT
INFORMATION SECURITY SERVICES

Define Information Security Team	• CISO • Assign security responsibilities to key personnel • Security Engineers & DevOps
Cartography	• Identify Information Assets. This may include assets related to PII, PHI, etc. (Data, Software, Hardware) • Identify their dependencies • Identify the core business requirements • Identify key suppliers
Conduct Readiness Assessment	• Map ISO 27001 & NIST controls with AICPA TSC requirements, ISO 27017, ISO 27018, ISO 27701, • Identify existing controls and find grey areas
Evaluate Key suppliers	• Evaluate their technical controls (TFA, Encryption, Backup, remote access etc.) • Evaluate Support Services & SLAs & DPA • Compliance with applicable regulation (i.e. GDPR, CCPA, NERC CIP, etc.)
Conduct Risk Assessment & Risk Treatment Plan	• Conduct Impact Assessment • Identify potential threats • Evaluate vulnerabilities • Propose Mitigation Actions
Develop technical & organizational controls	• Security Policies & Proceudres • SLAs with key suppliers • DPA with data processors • Hardening and automation as possible
Develop Contingency Plan	• Identify recovery priorities • Identify dependencies • Establish communication lines (internally and with the key suppliers) • Create Runbooks in case of unwanted event
Conduct Training & Awareness Programs	• Security Policies & Procedures • Remote work and Business continuity scenarios
Monitor, audit, and update security measures on an ongoing basis	• Internal Audits • Review

Mapping of Standards

ict PROTECT
INFORMATION SECURITY SERVICES

Mapping of Standards					
Standard	**Purpose**	**Information**	**Controls**	**Target**	**Certification**
HIPAA	Standard for **sensitive patient data protection**.	Protection of Protected Health Information and Electronic Protected Health Information.	Privacy, Security and Breach Notification Rules for PHI and ePHI	Covered Entities and Business Associates	No certification is endorsed
ISO 27017	Standard for **cloud service customers** and **cloud service providers**	Protection of Information stored in the cloud	Based on ISO/IEC 27001, 27002 security controls. Provides additional controls to address cloud-specific information security threats and risks considerations.	Cloud Service Providers and Cloud Service Customers	ISO certification is endorsed
ISO 27018	Standard for privacy of Personally Identifiable Information **(PII) stored in the cloud**	Protection of Personally Identifiable Information (PII) stored in the cloud	Based on ISO/IEC 27001, 27002 security controls. Emphasizes in additional controls to increase the level of protection of personal data in cloud services.	PII Controller, PII Processor	ISO certification is endorsed
ISO 27701	Standard for an effective **Privacy Information Management System**	Protection of Personally Identifiable Information (PII)	Based on ISO/IEC 27001, 27002 security controls. Provides additional controls for PII Controllers and PII Processors	PII Controller, PII Processor	ISO certification is endorsed (ISO 27001 is prerequisite)
SOC 2 (AICPA TSC)	Standard to help Organizations protect customer information and **data stored in cloud-based infrastructures**.	Protection of Customers data	SOC 2: focus on Information and IT Security related to Security, Availability, Processing, Integrity, Confidentiality and Privacy. SOC 3: same with SOC 2 but for public distribution	Organizations that process customers data in cloud services	SOC 2 Report is endorsed

Let’s do business

info@ictprotect.com

ict PROTECT
INFORMATION SECURITY SERVICES