ACS-2821-001

Information Security in Business

Information Security Principles

ACS-2821-001 – Slides Used In The Course

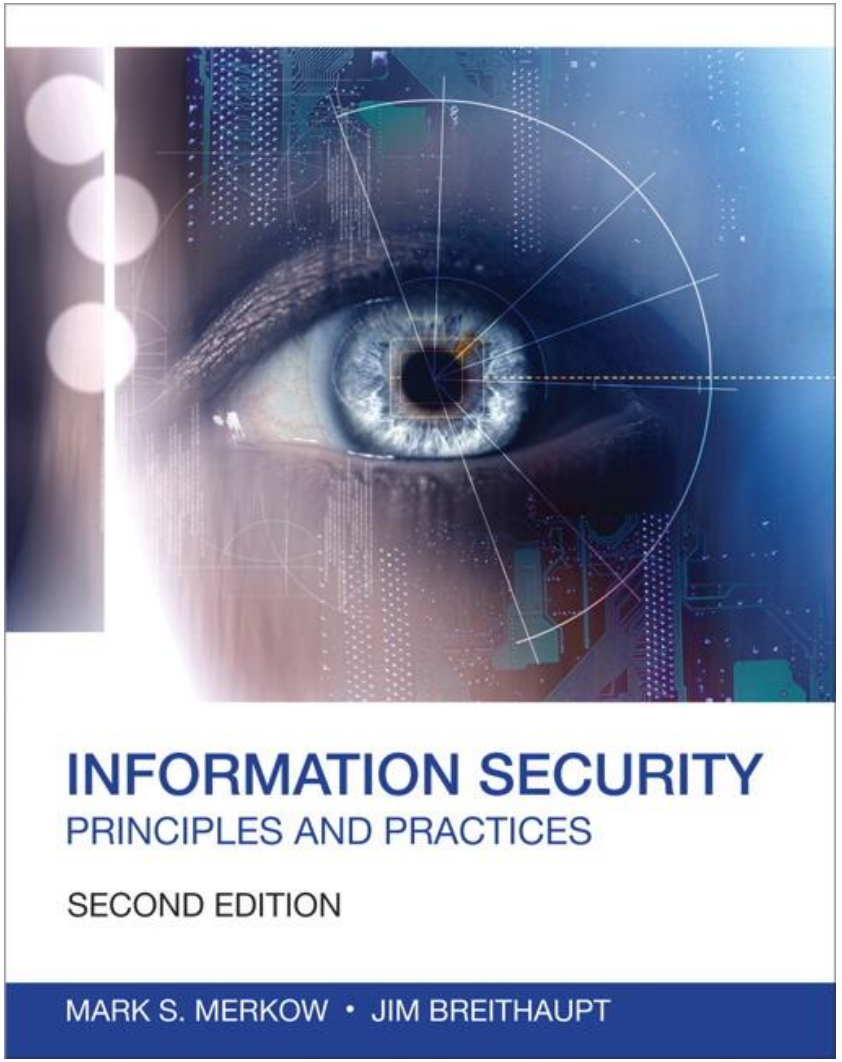
THE UNIVERSITY OF WINNIPEG

A note on the use of these slides:

These slides has been adopted and/or modified from the original for the use in this course. The author of the text have make these slides available to all (faculty, students, readers) and they obviously represent a *lot* of work on their part.

In return for use, please:

- If slides are being used (e.g., in a class) that the source be mentioned (after all, the author like people to use our book!)
- If any slides are being posted on a www site, note that they are adapted from (or perhaps identical to) the author original slides, and note their copyright of this material.



Objectives

- Build an awareness of 12 basic principles of information security
- Distinguish among the three main security goals
- Learn how to design and apply the principle of “Defense in Depth”
- Comprehend human vulnerabilities are security systems
- Explain the difference between functional and assurance requirements
- Comprehend the fallacy of security through obscurity
- Comprehend the importance of risk analysis and risk management tools and techniques
- Determine which side of open disclosure debate you would take

- Best security specialists combine practical knowledge and technical skills with understanding of human nature
  - No two systems or situations are identical, and there are no cookbooks to consult on how to solve security problems
  - Situational Awareness
    - Understand the organization environment
    - Knowledge of potential threats
    - Understand Technologies and their security impact
    - Understand the nature of the business

There Is No Such Thing as Absolute Security

- Given enough time, tools, skills, and inclination, a hacker can break through any security measure
- Security testing can buy additional time so the attackers are caught in the act
- Example - APT attack – Advance Persistent Attack

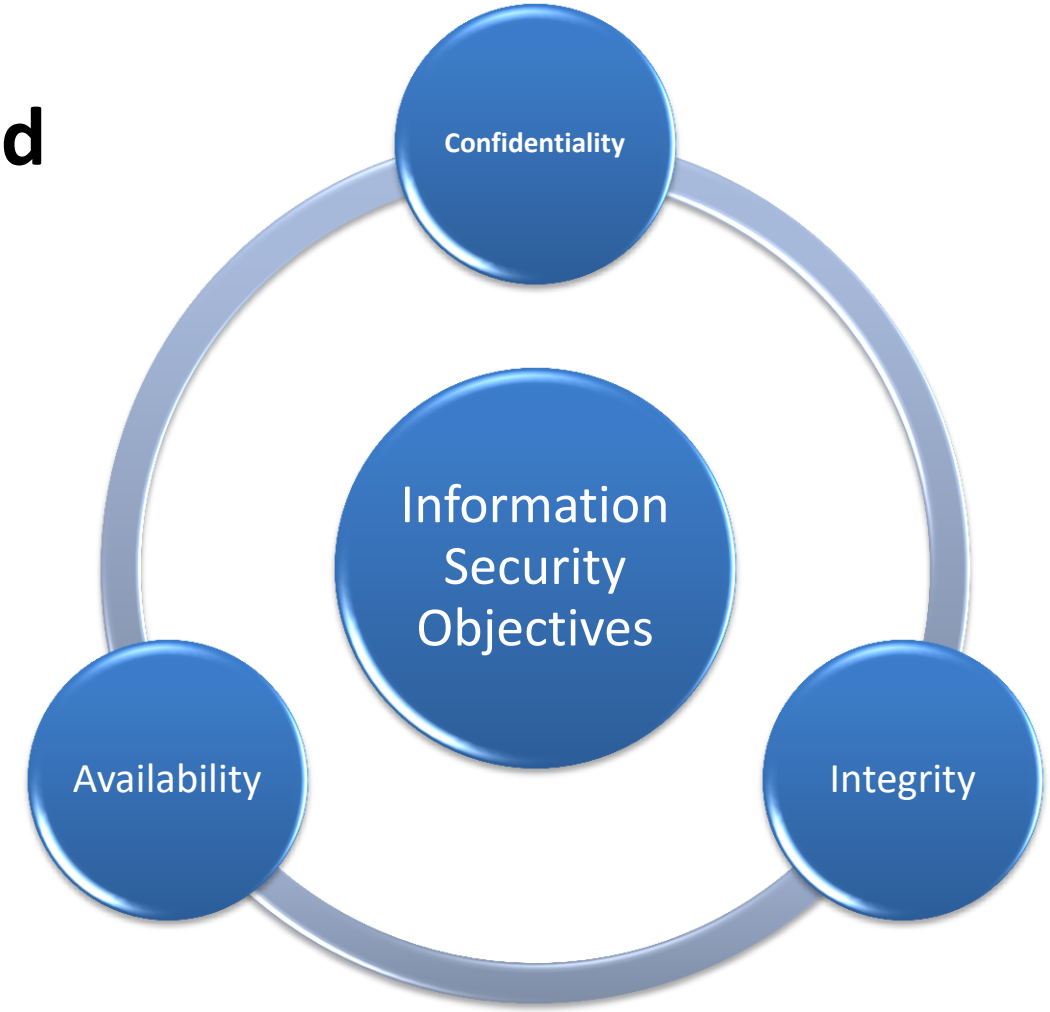
The Three Security Goals Are Confidentiality, Integrity, and Availability

- All information security measures try to address at least one of the three goals:
  - Confidentiality
  - Integrity
  - Availability
- Some security specialist added:
  - Accountability
  - Authenticity

InfoSec Principle 2 cont.

THE UNIVERSITY OF WINNIPEG

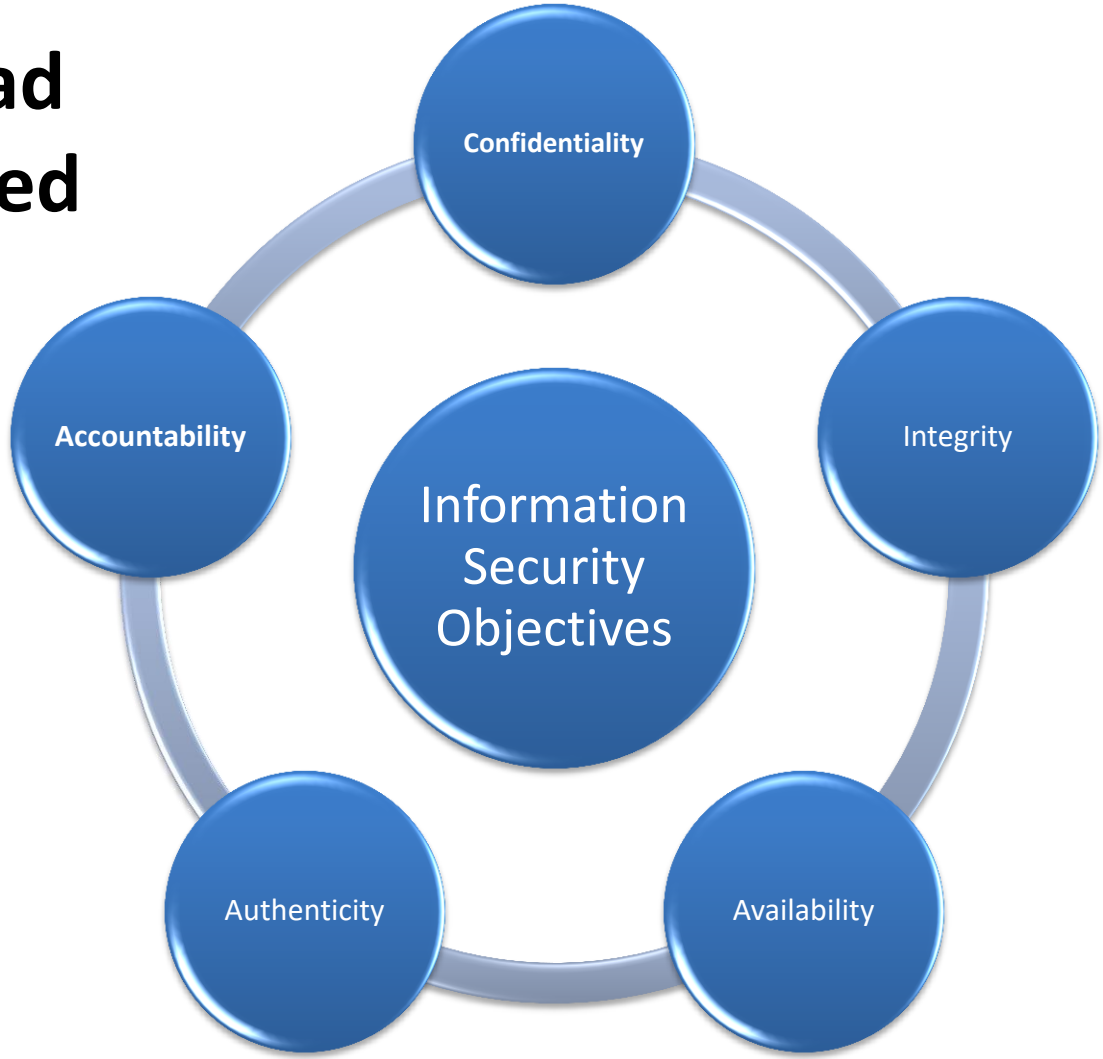
CIA triad



InfoSec Principle 2 cont.

THE UNIVERSITY OF WINNIPEG

CIA triad Modified



InfoSec Principle 2 cont.

- **Confidentiality**
  - Confidentiality models are primarily intended to ensure that no unauthorized access to information is permitted and that accidental disclosure of sensitive information is not possible
- **Integrity**
  - Integrity models keep data pure and trustworthy by protecting system data from intentional and accidental changes
- **Availability**
  - Availability models keep data and resources available for authorized use during denial-of-service attacks, natural disasters, and equipment failures

InfoSec Principle 2 cont.

THE UNIVERSITY OF WINNIPEG

- **Authenticity**
  - Ensure validity of a transmission, a message, or message originator and that it is from a trusted source.
- **Accountability**
  - Supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action
  - Keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes

Defense in Depth as Strategy

- Defense in depth
  - Involves implemented security in overlapping layers that provide the three elements needed to secure assets: prevention, detection, and response
  - The weaknesses of one security layer are offset by the strengths of two or more layers

InfoSec Principle 3 cont.

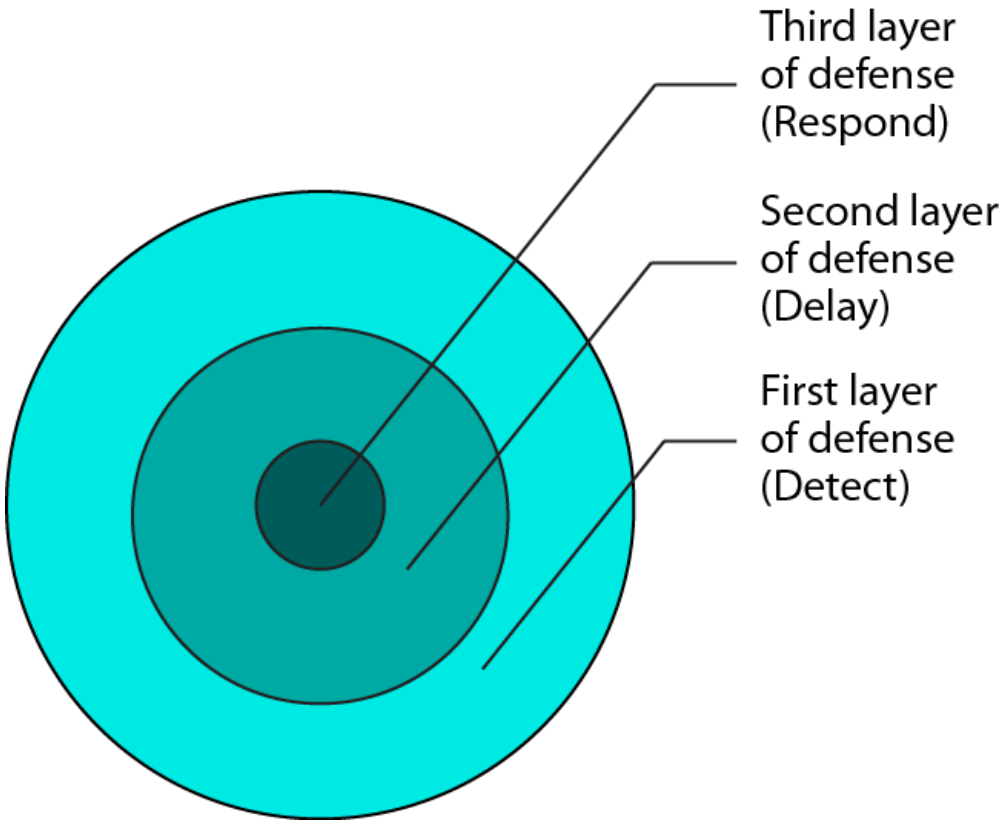
THE UNIVERSITY OF WINNIPEG

Defense in Depth Strategies:

- CONCENTRIC RINGS
  - Creates a series of nested layers.
  - Each layer delays and provides opportunities to detect the attack.
- OVERLAPPING REDUNDANCY
  - Two or more controls that work in parallel to protect an asset.
  - Providing multiple, overlapping points of detection.
  - Most effective when each control is different.
- SEGREGATION OR COMPARTMENTALIZATION
  - Compartmentalizes access to an asset
  - Need two or more processes, controls or individuals to access the asset.
  - Effective in protecting very high value assets or in environments where trust is an issue.

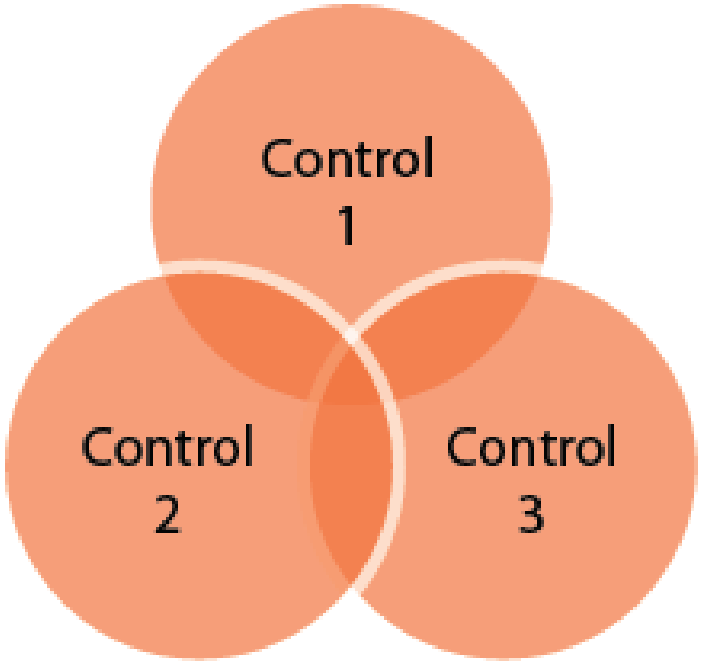
InfoSec Principle 3 cont.

CONCENTRIC RINGS



InfoSec Principle 3 cont.

OVERLAPPING REDUNDANCY



InfoSec Principle 3 cont.

SEGREGATION OR COMPARTMENTALIZATION

InfoSec Principle 3 cont.

THE UNIVERSITY OF WINNIPEG

Examples:

- Multiple firewalls at the perimeter from different vendor
- Use firewall(s) to separate the R&D department
- Intrusion Detection System/Intrusion Prevention System sensors through out the network
- Data loss prevention software
- Backups
- Virtue Local Area Network – VLAN
- Anti-virus software
- The list goes on…

InfoSec Principle 4

InfoSec Principle 4

When Left on Their Own, People Tend to Make the Worst Security Decisions

- Takes little to convince someone to give up their credentials in exchange for trivial or worthless goods
- Many people are easily convinced to double-click the attachment or links inside emails

Subject: Here you have, ;o)
Message body: Hi: Check This!
Attachment: AnnaKournikova.jpg.vbs

InfoSec Principle 4

THE UNIVERSITY OF WINNIPEG

Social Engineering

- Psychological manipulation of people into performing actions or divulging confidential information.
- Phishing is the most common attack method. Different phishing technique, for example:
  - Spear Phishing
    - Is directed to specific individuals or companies
  - Clone Phishing
    - Create an almost identical or cloned of a legitimate, and previously delivered email that contain an attachment or link. The attachment or link is being replaced by with a malicious version and then re-sent with an email address spoofed to appear it is from the original sender
  - Whaling
    - Is directed specifically at senior executives and other high-profile target
- Other social engineering technique - Watering Hole, Tailgating

InfoSec Principle 5

Computer Security Depends on Two Types of Requirements: Functional and Assurance

- Functional requirements
  - Describe what a system should do
- Assurance requirements
  - Describe how functional requirements should be implemented and tested
  - Does the system do the right things in the right way?
    - Verification: The process of confirming that one or more predetermined requirements or specifications are met
    - Validation: A determination of the correctness or quality of the mechanisms used in meeting the needs

InfoSec Principle 6

THE UNIVERSITY OF WINNIPEG

Security Through Obscurity Is Not an Answer

- Many people believe that if hackers don't know how software is secured, security is better
  - Although this seems logical, it's actually untrue
- Obscuring security leads to a false sense of security, which is often more dangerous than not addressing security at all

InfoSec Principle 6 cont.

THE UNIVERSITY OF WINNIPEG

Cryptography is a good example

- All cryptography algorithms are published and can be obtained.
  - RSA (Rivest–Shamir–Adleman) is a public-key cryptosystem.
  - The cryptosystems has two keys for encryption and decryption.
  - One key is call a private key, and one is call a public key.
  - In RSA, the two keys or asymmetry keys is based on the practical difficulty of factorization of the product of two large prime numbers.
  - The importance here is not the algorithm but the management of the two keys of the cryptosystem.

InfoSec Principle 7

THE UNIVERSITY OF WINNIPEG

Security = Risk Management

- Security is not concerned with eliminating all threats within a system or facility but with *eliminating known threats and minimizing losses* if an attacker succeeds in exploiting a vulnerability
- Spending more on security than the cost of an asset is a waste of resources – cost vs benefit
- Risk assessment and risk analysis are used to *place an economic value on assets to best determine appropriate countermeasures* that protect them from losses

InfoSec Principle 7 cont.

- Two factors to determine risk
  - What is the consequence of a loss?
  - What is the likelihood the loss will occur?
- Consequences/likelihood matrix

Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	High	High	Extreme	Extreme	Extreme
Likely	Moderate	High	High	Extreme	Extreme
Moderate	Low	Moderate	High	Extreme	Extreme
Unlikely	Low	Low	Moderate	High	Extreme
Rare	Low	Low	Moderate	High	High

InfoSec Principle 7 cont.

- Vulnerability
  - A known problem within a system or program
- Exploit
  - A program or a “cookbook” on how to take advantage of a specific vulnerability
- Attacker
  - The link between a vulnerability and an exploit

InfoSec Principle 8

The Three Types of Security Controls Are Preventative, Detective, and Responsive

- Remember in *InfoSec Principle 3* we mention that in Defense In Depth, we want to be able to *prevent, detect* and *response* to threat.
- A security mechanism serves a purpose by **preventing a compromise, detecting that a compromise or compromise attempt** is underway, or **responding to a compromise** while it is happening or after it has been discovered.

InfoSec Principle 8

THE UNIVERSITY OF WINNIPEG

Preventive

- Firewalls
- Intrusion Prevention Systems (IPS)
- Security Guards
- Biometric Access Control
- Using Encryption
- Video Surveillance
- Fences
- Strong Authentication
- Locks
- Mantraps
- Antivirus Software

Detection

- Intrusion Detection Systems (IDS)
- Alarms
- Lights
- Motion Detectors
- Security Guards
- Video Surveillance
- Logs and Audit Trails
- Enforcing Staff Vacations

Responding

- Restoring operating system or data from a recent backup
- Updating an outdated antivirus
- Installing a fix or patch
- Disaster Recovery Site
- System and Data backups
- High Availability

InfoSec Principle 9

Complexity Is the Enemy of Security

- The more complex a system gets, the harder it is to secure.

InfoSec Principle 10

THE UNIVERSITY OF WINNIPEG

Fear, Uncertainty, and Doubt (FUD) Do Not Work in Selling Security

- Information security managers must justify all investments in security using techniques of the trade.
- When spending resources can be justified with good, solid business rationale, security requests are rarely denied.

InfoSec Principle 11

THE UNIVERSITY OF WINNIPEG

People, Process, and Technology Are All Needed to Adequately Secure a System or Facility

- People controls
  - Dual control and separation of duties
- Process controls
  - Different people can perform the same operation the same way every time
- Technology alone without people and process controls can fail
- People, process, and technology controls are essential elements of security practices including operations security, applications development security, physical security, and cryptography
- Security is everyone business

InfoSec Principle 12

THE UNIVERSITY OF WINNIPEG

Open Disclosure of Vulnerabilities Is Good for Security!

- Keeping a given vulnerability secret from users and from the software developer can only lead to a false sense of security
- The need to know trumps the need to keep secrets to give users the right to protect themselves

InfoSec Principle 12

- Ransomware - WannaCry is a good example on this principle.
- This one attack spread across the globe like a wildfire.
- Infecting hospital systems in Ukraine to National Health Service in the UK and radio stations in the United States.
- In total it infected more than 400,000 systems across the world.
- The ransomware exploited an already-discovered vulnerability in the SMB protocol.
- The attackers used ETERNALBLUE, one of those NSA-built tools that were leaked by Shadow Brokers.
- Prior to this leak by Shadow Brokers in March 2017, Microsoft had released an update on March 14, 2017, for patching the vulnerability and marked it as critical, but it were only for the latest version of Window.
- Window XP system was not in the scope which Microsoft later provide security patch in view of the seriousness with this vulnerability.

Summary

- Computer security specialists must not only know the technical side of their jobs but also must understand the principles behind information security
- These principles are mixed and matched to describe why certain security functions and operations exist in the real world of IT

ACS-2821-001 – Questions?