Appendix A: Objectives and Locations

Students can use this appendix as a study guide to locate content within this course that corresponds to specific CIW and AIP objectives.

Occasional repetition among objectives reflects an overlap in the two programs. In many cases, multiple CIW objectives fulfill one AIP objective.

Objective	CIW	AIP	Lesson and Section(s)
Define security.	✓		**Lesson 1: What is Security?** - What Is Security?
Explain the need for network security.	✓		**Lesson 1: What is Security?** - What Is the Risk? - Hacker Statistics
Describe the potential risk factors for data security. [AIP]	✓	✓	**Lesson 1: What Is Security?** - What Is the Risk? - The Myth of 100 Percent Security
Summarize risk factors, including improper authentication. [AIP]	✓	✓	**Lesson 1: What Is Security?** - What Is the Risk? - The Myth of 100 Percent Security
Identify security-related organizations, warning services, and certifications. [AIP]	✓	✓	**Lesson 1: What Is Security?** **Security Standards** **Appendix A: Internet Security Resources**
Identify resources that need security.	✓		**Lesson 1: What is Security?** - What You Are Trying to Protect
Identify the two general security threat types.	✓		**Lesson 1: What is Security?** - Who Is the Threat?

Objective	CIW	AIP	Lesson and Section(s)
Describe how increased security mechanisms can result in increased latency. [AIP]	✓	✓	**Lesson 2: Elements of Security** - Security Tradeoffs and Drawbacks
Identify the importance of a security policy. [AIP]	✓	✓	**Lesson 2: Elements of Security** - The Security Policy
Formulate the basics of an effective security policy.	✓		**Lesson 2: Elements of Security** - Elements of Security - The Security Policy
Identify the key user authentication methods.	✓		**Lesson 2: Elements of Security** - Authentication - Specific Authentication Techniques
Explain the need for access control methods.	✓		**Lesson 2: Elements of Security** - Access Control - Lab 2-1: Viewing and modifying default access control settings in Windows 2000
Describe the function of an access control list and an execution control list.	✓		**Lesson 2: Elements of Security** - Access Control - Optional Lab 2-1: Creating an access control list for Apache Server
Understand execution control lists.	✓		**Lesson 2: Elements of Security** - Execution Control Lists - Lab 2-2: Viewing the effects of hostile JavaScript in Netscape Navigator - Lab 2-3: Configuring execution control lists in Windows 2000 - Lab 2-4: Creating an execution control list for the su command in Linux
List the three main encryption methods used in internetworking.	✓		**Lesson 2: Elements of Security** - Encryption
Explain the need for auditing.	✓		**Lesson 2: Elements of Security** - Auditing
Consider ease of use when choosing security equipment and software.	✓		**Lesson 2: Elements of Security** - Security Tradeoffs and Drawbacks
Identify security factors in regards to sending unencrypted data across the network. [AIP]	✓	✓	**Lesson 2: Elements of Security** - Encryption

Objective	CIW	AIP	Lesson and Section(s)
Describe the usefulness of parallel processing in regards to cryptography. [AIP]	✓	✓	**Lesson 3: Applied Encryption** - Rounds, Parallelization and Strong Encryption
Explain the need for encryption in enterprise networks. [AIP]	✓	✓	**Lesson 3: Applied Encryption** - Creating Trust Relationships
Explain the impact of encryption protocols and procedures upon system performance. [AIP]	✓	✓	**Lesson 3: Applied Encryption** - Symmetric-Key Encryption - Symmetric Algorithms - Asymmetric Encryption - Hash Encryption
Create a trust relationship using public-key cryptography.	✓		**Lesson 3: Applied Encryption** - Creating Trust Relationships
List specific forms of symmetric, asymmetric and hash encryption.	✓		**Lesson 3: Applied Encryption** - Symmetric-Key Encryption - Symmetric Algorithms - Asymmetric Encryption - Hash Encryption - Applied Encryption Processes
Deploy PGP in Windows NT/2000 and Linux.	✓		**Lesson 3: Applied Encryption** - Lab 3-1: Reviewing symmetric encryption algorithms - Optional Lab 3-1: Using MD5sum to create checksums in Red Hat Linux - Lab 3-2: Installing PGP 6.5.8 in Windows 2000 - Generating a key pair using PGP for Windows 2000 - Lab 3-4: Exporting and signing public keys using PGP for Windows 2000 - Exchanging encrypted messages using PGP for Windows 2000 - Lab 3-7: Encrypting files with PGP in Windows 2000 - Optional Lab 3-2: Generating a key pair using gpg for Red Hat Linux
Configure a Windows 2000 server to support IPSec.	✓		**Appendix E: Configuring a Windows 2000 Server to use IPsec** - Lab E-1: Obtaining an IPsec certificate from a CA. - Lab E-2: Enabling IPSec on your host.

Objective	CIW	AIP	Lesson and Section(s)
Describe specific types of security attacks.	✓		**Lesson 4: Types of Attacks** - Brute-Force and Dictionary Attacks - System Bugs and Back Doors - Buffer overflow - Trojans and root kits - Social Engineering and Non-direct Attacks - Denial of service attacks (including Distributed Denial of Service attacks). - Spoofing attacks. - Viruses - Man in the middle attacks.
Describe a brute-force attack. **AIP**	✓	✓	**Lesson 4: Types of Attacks** - Brute-Force and Dictionary Attacks
Explain a dictionary attack. **AIP**	✓	✓	**Lesson 4: Types of Attacks** - Front-Door and Brute-Force Attacks
Identify routing issues and security. **AIP**	✓	✓	**Lesson 4: Types of Attacks** - Social Engineering and Non-direct Attacks **Lesson 8: Firewalls** - Circuit-Level Gateways - Application-Level Gateways **Lesson 9: Levels of Firewall Protection** - Hardware Issues
Determine the causes and results of a denial-of-service (DOS) attack. **AIP**	✓	✓	**Lesson 4: Types of Attacks** - Why? - Social Engineering and Non-Direct Attacks **Lesson 6: Protocol Layers and Security** - Network Layer - Application Layer **Lesson 7: Securing Resources** - Protecting TCP/IP Services - Simple Mail Transfer Protocol (SMTP) **Lesson 11: Incident Response** - Execute the Response Plan **Appendix B: Commercial Products Used in This Course**

Objective	CIW	AIP	Lesson and Section(s)
Recognize attack incidents. [AIP]	✓	✓	**Lesson 4: Types of Attacks** - Brute-Force and Dictionary Attacks - Bugs and Back Doors - Social Engineering and Non-direct Attacks
Describe the universal guidelines and principles for effective network security.	✓		**Lesson 5: General Security Principles** - Be Paranoid - You Must Have a Security Policy - No System or Technique Stands Alone - Minimize the Damage - Deploy Companywide Enforcement - Provide Training - Use an Integrated Security Strategy - Place Equipment According to Needs - Identify Security Business Issues - Consider Physical Security
Discuss amortization and chargeback issues in regards to network security architectures. [AIP]	✓	✓	**Lesson 5: General Security Principles** - Identify Security Business Issues
Use universal guidelines to create effective specific solutions.	✓		**Lesson 5: General Security Principles** - You Must Have a Security Policy - No System or Technique Stands Alone - Minimize the Damage - Deploy Companywide Enforcement - Provide Training - Use an Integrated Security Strategy - Place Equipment According to Needs - Identify Security Business Issues - Consider Physical Security - Optional Lab 5-2: Optional Lab 5-2: Exploiting and protecting Red Hat Linux single-boot mode - Lab 5-1: Conducting a physical attack against a Windows 2000 server

Objective	CIW	AIP	Lesson and Section(s)
Identify potential threats at different layers of the TCP/IP stack.	✓		**Lesson 6: Protocol Layers and Security** - TCP/IP and Network Security - Physical Layer - Network Layer - Transport Layer - Application Layer - Lab 6-1: Enabling TCP/IP filtering on Windows 2000 - Optional Lab 6-1: Using a port listener on Windows 2000 to conduct a traceback
Consistently apply security principles.	✓		**Lesson 7: Securing Resources** - Implementing Security - Protecting TCP/IP Services - Optional Lab 7-1: Executing arbitrary code in Apache Server - Lab 7-1: Securing a Windows 2000Web server - Lab 7-2: Securing the FTP service
Describe how to protect your operating systems, routers, and equipment against physical attacks. **AIP**	✓	✓	**Lesson 7: Securing Resources** - Implementing Security - Resources and Services
Secure TCP/IP Services, including HTTP and FTP.	✓		**Lesson 7: Securing Resources** - Protecting TCP/IP Services - Lab 7-2: Securing the FTP service
Describe the importance of testing and evaluating systems and services.	✓		**Lesson 7: Securing Resources** - Security Testing Software
Discuss network security management applications, including network scanners, operating system add-ons, and log analysis tools.	✓		**Lesson 7: Securing Resources** - Security Testing Software - Lab 7-3: Deploying simple network scanners - Lab 7-4: Scanning systems using Red Hat Linux
Define and describe firewalls.	✓		**Lesson 8: Firewalls** - Definition and Description of a Firewall
Describe the role a firewall plays in a company's security policy.	✓		**Lesson 8: Firewalls** - The Role of a Firewall

Objective	CIW	AIP	Lesson and Section(s)
Define common firewall terms.	✓		**Lesson 8: Firewalls** - Firewall Terminology
Describe packet filters and their features.	✓		**Lesson 8: Firewalls** - Packet Filters - Packet Filter Advantages and Disadvantages - Creating packet filter rules - Lab 8-2: Configuring packet filtering rules - Optional Lab 8-1: Using the `ipchains` command to create a personal firewall in Linux - Optional Lab 8-2: Using the `iptables` command to create a personal firewall in Linux
Describe circuit-level gateways and their features.	✓		**Lesson 8: Firewalls** - Circuit-level Gateways
Describe and configure an application-level gateway.	✓		**Lesson 8: Firewalls** - Application-level Gateways
Describe the features of a packet-filtering firewall, including rules and stateful multiplayer inspection. **AIP**	✓	✓	**Lesson 8: Firewalls** - Firewall Terminology - Packet Filters - Packet Filter Advantages and Disadvantages
Describe the fundamental features of a proxy-based firewall, including service redirection, service passing, and gateway daemons. **AIP**	✓	✓	**Lesson 8: Firewalls** - Firewall Terminology - Proxy Servers - Web Proxies - Application-Level Gateways - Lab 8-1: Installing WinRoute in Windows 2000 - Lab 8-3: Configuring a proxy server in Windows 2000 - Advanced Features
Describe application-level gateways and their features. **AIP**	✓	✓	**Lesson 8: Firewalls** - Firewall Terminology - Application-Level Gateways - Lab 8-3: Configuring a proxy server in Windows 2000
List the features of a circuit-level gateway. **AIP**	✓	✓	**Lesson 8: Firewalls** - Firewall Terminology - Circuit-Level Gateways

Objective	CIW	AIP	Lesson and Section(s)
Understand the importance of proxy caching in regards to performance. **AIP**	✓	✓	**Lesson 8: Firewalls** - Application-Level Gateways **Lesson 9: Levels of Firewall Protection** - Hardware Issues
Understand and implement proxy-level firewall security. **AIP**	✓	✓	**Lesson 8: Firewalls** - Firewall Terminology - Proxy Servers - Web Proxies - Application-level Gateways
Plan a firewall system that incorporates several levels of protection.	✓		**Lesson 9: Levels of Firewall Protection** - Firewall Strategies and Goals - Building a Firewall
Describe the four types of firewall systems design and their degrees of security.	✓		**Lesson 9: Levels of Firewall Protection** - Common Firewall Designs
Implement a packet-filtering firewall.	✓		**Lesson 9: Levels of Firewall Protection** - Lab 9-1: Creating an internal network with WinRoute *(instructor-led)* - Lab 9-2: Establishing a packet filter *(instructor-led)* - Lab 9-3: Denying HTTP access *(instructor-led)* - Lab 9-4: Configuring an FTP packet-filtering rule for a specific host *(instructor-led)*
Customize your network to manage hacker activity.	✓		**Lesson 10: Detecting and Distracting Hackers** - Proactive Detection - Distracting the Hacker - Lab 10-1: Setting a logon tripwire script in Windows 2000 - Optional Lab 10-1 Optional Lab 10-1: Using Tripwire for Linux - Punishing the Hacker
Implement proactive detection.	✓		**Lesson 10: Detecting and Distracting Hackers** - Proactive Detection
Distract hackers and contain their activity.	✓		**Lesson 10: Detecting and Distracting Hackers** - Punishing the Hacker
Set traps.	✓		**Lesson 10: Detecting and Distracting Hackers** - Punishing the Hacker

Objective	CIW	AIP	Lesson and Section(s)
Deploy Tripwire for Linux.	✓		**Lesson 10: Detecting and Distracting Hackers** - Optional Lab 10-1: Using Tripwire for Linux
Respond appropriately to a security breach.	✓		**Lesson 11: Incident Response** - Decide Ahead of Time - Do Not Panic - Document Everything - Assess the Situation - Stop or Contain Activity - Execute the Response Plan - Analyze and Learn
Identify some of the security organizations that can help you in case your system is attacked. **AIP**	✓	✓	**Lesson 11: Incident Response** - Execute the Response Plan
Subscribe to respected security alerting organizations. **AIP**	✓	✓	**Lesson 11: Incident Response** - Lab 11-1: Subscribing to security mailing lists
Understand the appropriate authorities to contact regarding theft of data and assorted attacks. **AIP**	✓	✓	**Appendix A: Internet Security Resources**

AIP This symbol indicates an objective developed by the Association of Internet Professionals (AIP) (*www.accredit.net/accredited.html*).

