CDDS
DNSSEC Implementation & Operations

Overview
DNSSEC is an included component of the DNS protocol and a critical element of your complete DNS security strategy. Generic DNSSEC courses teach the protocol basics. This Infoblox DNSSEC course teaches you how the protocol works, the implementation and operations tasks you need to know, how to troubleshoot your DNSSEC environment, and how DNSSEC integrates with your complete DNS security strategy. In this course you will establish detailed protocol knowledge in preparation for the deployment, operations and maintenance, and troubleshooting of your DNSSEC environment. You will learn about DNS protocol changes and network requirements related to DNSSEC, operations and maintenance tasks such as key management, threats against DNSSEC, troubleshooting techniques and available GUI and CLI tools, and best practices.

Target Audience
US Government agencies are required to deploy DNSSEC, which is a new protocol to users. This advanced-level course is for teams responsible for DNS and DNS security architecture, implementation and operations.

Course Length
2 days

Prerequisites
Attendees should have completed the Core DDI Configuration & Administration (CDCA) or have equivalent hands-on DDI experience.

Style
Lecture and hands-on lab exercises using a break-fix approach to troubleshoot and resolve common operation issues.

Delivery
- Instructor-led
- Virtual instructor led

Max Class Size
8 attendees

Topics
Day 1

- Introduction to DNSSEC
- DNSSEC Protocol Deep Dive
- New DNSSEC Record Types
- Implementing Trust Anchor

Day 2

- Managing DNSSEC Keys
- Working with Proof of Non-Existence
- Critical Network Considerations
- Common Threats and Mitigations
- Best Practices for Operations

Accreditation
Core DDI DNSSEC Ops & Troubleshooting (CDDS) attendance on completion of course.

Training Credits
20