Strengthening the Security of the Defense Industrial Base (DIB) – U.S. Defense Contractors

Contents

U.S. Commercial and Global Enterprise

The challenge

Your company is working to deliver capabilities to the DoD, and you're constantly battling to keep it secure against active adversaries who are well- funded and endlessly patient and that's on top of everything else—new regulations, new mandates, tight budgets, and the revolving door of security talent. You don't have time and resources to waste stitching multiple security and networking products that do not easily fit together. Challenges abound such as, keeping an accurate device inventory, identifying, and providing least-privileged access to **all** users, **all** applications, and **all** devices—while simultaneously remediating vulnerabilities, identifying threats, and being able to respond to any incident at a moment's notice to protect the Government's information and your company data. You're constantly juggling risk management for the whole business while simultaneously empowering your product teams to move fast.

The new paradigm in security

The DoD's Cybersecurity Maturity Model Certification (CMMC) program represents a **new paradigm** for DoD to require effective cybersecurity practices and processes from the Defense Industrial Base (DIB). Correspondingly, it is time to adopt a **new security paradigm** for your enterprise. One that reduces risk and makes compliance easier as an integrated solution. One that fuses your business and security architecture. One that enables you and your workforce to focus valuable time and energy on delivering capabilities to the Nation—always with security.

Like the CMMC's approach, creating a **new security paradigm** means breaking with convention. Cisco is in the business of building an integrated platform, bringing together your currently siloed products. We believe in delivering end-to-end, threat-informed, streamlined security and networking solutions designed to **work together** with open standards and interfaces. Our goal is for you to be secure and compliant with less effort. As the largest Cybersecurity company in the world—**protecting 100% of Fortune 100**, Cisco has the breadth and depth of knowledge to solve platform-level security and networking challenges that span **IT, OT, campus, data center, network, cloud, internet, email, endpoints, and everywhere in between**. All backed by Cisco Talos threat intelligence teams, world-class researchers, analysts, and engineers providing industry-leading visibility, actionable intelligence, and vulnerability research to protect your company's enterprise from known APTs, emerging threats or any malicious intent.

What is CMMC?

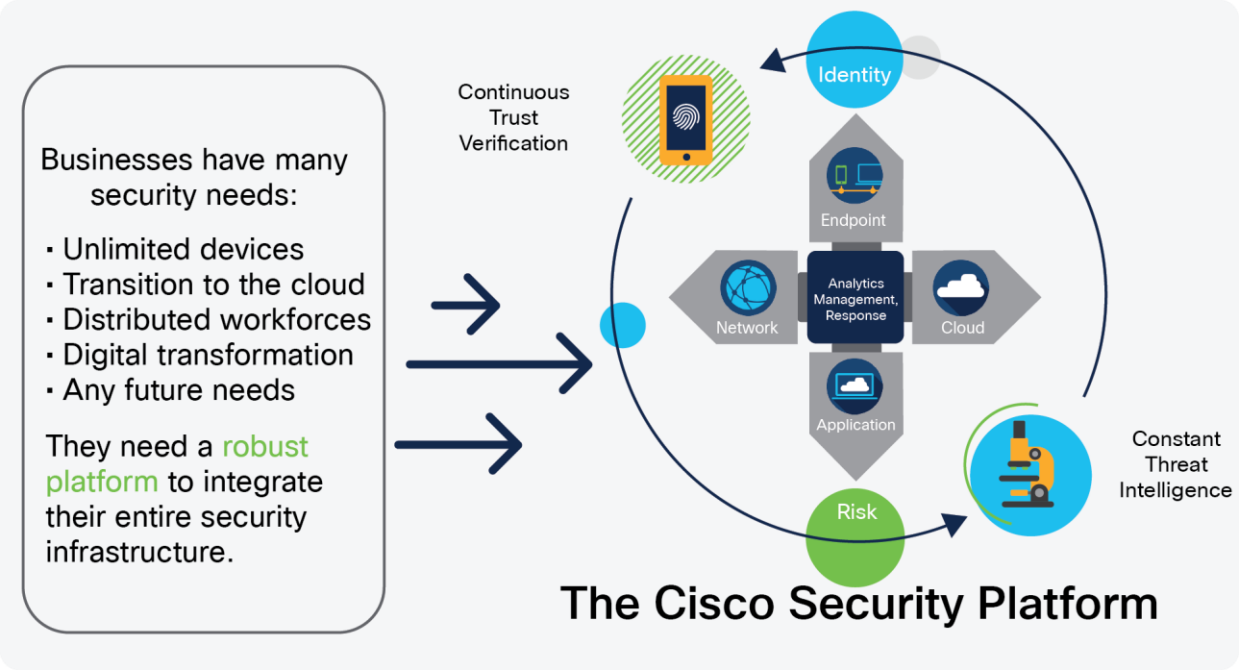
The DoD published CMMC version 1.02 on March 18, 2020. The CMMC consists of 5 maturity levels across 17 capability domains encompassing 43 capabilities, which were developed from the DFARS clause 252.204-7012 ("Safeguarding of Covered Defense Information and Cyber Incident Reporting") and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. DIB contractors must meet CMMC at a specified level to respond to a selected number of forthcoming Requests for Proposals starting in the Fall of 2020—with a goal of being integrated in all new DoD contracts by 2026.

Most companies that are a part of the DIB are familiar with many CMMC practices due to this relationship with NIST SP 800-171 and the current DFARS clause 252-204.7012. In addition to these requirements, the practices in the CMMC model also incorporate frameworks from other sources as described in the CMMC Appendices. However, different from the previous NIST 800-171 and DFARS clause model, in this **new paradigm**, compliance with the CMMC will be verified by an accredited third-party assessor to determine if the DIB company meets the requisite maturity level specified in the DoD contract.

Platform matters—breaking security and networking silos

Our goals are to enable you: to protect the Government's information; to protect and efficiently operate your company's enterprise; and to ensure compliance and security—all with greater visibility and less effort. We believe that is only possible with a platform approach supported by open, industry-standard integrations. And that a platform should augment and bring together your current capabilities to deliver advantages whether you start with one product or an entire architecture.

As the global leader in security and networking, Cisco is uniquely positioned to embed security into your network and architecture at scale via an open-standards, integrated platform—not through bolt-on, siloed products; we're committed to delivering an enhanced security experience and protecting the information and capabilities you are delivering to the Nation.



Cisco provides integrated solutions for the DIB to comply with CMMC

As the industry-recognized leader in Zero Trust Security and Architecture and leading solutions provider for the **DoD's Comply-to-Connect (C2C)** program, and the **Federal Government's Continuous Diagnostics and Mitigation (CDM)** program, Cisco offers the most expansive products and services offerings to address CMMC requirements. Designed to work together with an industry-standards-based open architecture, Cisco's platform connects your security tools to unify visibility, enable automation, and strengthen security across the network, users, endpoints, cloud, and applications. Cisco's product portfolio is already well-known for alignment and mapping to the technical areas of the **NIST Cybersecurity Framework's** desired outcomes and can help support an integrated solution across the technical requirements of the CMMC Domains as well. Cisco's comprehensive cybersecurity products and services portfolio defends DIB organizations against today's advanced threats—more easily and without "point solutions."

CMMC Domain Capabilities, Practices, and Processes	Cisco Products Can Be Applied to Many CMMC Capabilities, Practices, and Processes													
	Identity Services Engine (ISE)	Duo Adaptive MFA	TrustSec	Any Connect VPN	Umbrella DNS	Stealth-watch	Cyber Vision	Fire Power	Advanced Malware Protection (AMP)	Tetration	Meraki	Cisco SecureX and Threat Response	Talos Incident Response	Cisco Services
Access Control (AC)	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Identification and Authorization (IA)	■	■	■	■	■	■	■	■		■	■	■	■	■
Audit and Accountability (AU)	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Risk Management (RM)	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Configuration Management (CM)	■	■	■	■	■		■	■	■	■	■	■	■	■
Incident Response (IR)	■	■	■	■	■	■	■	■	■	■	■	■	■	■
System and Communication Protection (SC)	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Security Assessment (CA)	■	■	■	■	■	■	■	■	■	■	■	■	■	■
System and Info. Integrity (SI)	■					■	■	■	■	■	■	■	■	■
Situational Awareness (SA)					■	■		■	■		■	■	■	■
Asset Management (AM)	■			■			■	■				■		■
Maintenance (MA)	■	■							■					■
Media Protection (MP)	■								■			■		■
Recovery (RE)												■	■	■
Awareness and Training (AT)												■	■	■
Personal Security (PS)	Non-technical Cyber Capability													
Physical Protection (PE)	Non-technical Cyber Capability													

How Cisco Can Support CMMC compliance

An integrated, portfolio-based platform delivers more value than point-solution-based or single-technology-based platforms. An integrated, portfolio- based platform unifies visibility and enables automation by working together. For example, the following table highlights how some products and services could work together to satisfy practices and processes within several key CMMC Domains. When combined with Cisco's Digital Network Architecture (Cisco DNA), an open, extensible, software-driven architecture, you can integrate existing products and simplify enterprise operations while lowering costs and reducing your risk. Only Cisco provides a single network fabric that is powered by deep threat intelligence and integrated security.

The simplified table below provides a brief overview of the capabilities of several Cisco products that can support practices and processes associated with the following CMMC Domains:

- Access Control (AC)
- Ident. and Authentication (IA)
- Audit and Accountability (AU)
- Risk Management (RM)
- Incident Response (IR)
- Configuration Management (CM)
- Security Assessment (CA)
- System and Info. Integrity (SI)
- Situational Awareness (SA)
- Asset Management (AM)
- Recovery (RE)
- Awareness and Training (AT)

Cisco Identity Services Engine (ISE) connects user identity with device profiling, identification, IEEE 802.1X access, and authentication policy, ensuring that only authorized individuals with authorized devices can access only the systems and data that policy permits and that actions can be traced to individual users for audit and accountability. Upon alert from multiple sources or via an IETF-standards interface, quickly identifies the source of an incident and automatically quarantines the user/device. Integration with Stealthwatch anomalous traffic detection provides rapid incident response and forensics. ISE policy enforcement ensures that only authorized individuals with authorized devices can securely access only authorized systems and data and that actions can be tracked to individual users satisfying configuration management, security controls and requirements.

Cisco SecureX and Threat Response accelerate investigations by automating and aggregating threat intelligence and data across the security infrastructure—Cisco's and others' capabilities—into one unified view while collecting and storing key investigation information; and managing and documenting progress and findings. Administrators can implement corrective action directly from the interface; block suspicious files, domains, and more without having to log in to another product. Talos Incident Response provides proactive and reactive services to prepare, respond and recover from a breach. Direct access to the same threat intelligence available to Cisco and world-class emergency response capabilities – in addition to more than 350 threat researchers for questions and analysis and helps develop a security incident response process and plan; playbooks; tabletop exercises; compromise assessments; and conduct threat hunting.

Duo Adaptive Multi-Factor Authentication Access defines policies that limit application access to the users and devices according to distinct risk tolerance levels and can easily integrate with hundreds of applications in hybrid environments. Duo verifies the identity of all users with effective, two-factor authentication before granting access to corporate applications and resources and provides visibility into every device used to access corporate applications—whether or not the device is corporate-managed. Duo inspects all devices used to access corporate applications and resources, at the time of access, to determine security posture and trustworthiness and grants authorized users secure access to protected applications (on-premises or cloud-based). Duo also offers integration with OTP-based hard tokens and YubiKeys that meet FIPS 140-2 requirements.
CyberVision, developed for OT and IT with integration across Cisco's entire security portfolio, provides full visibility into Industrial Control Systems (ICS), including dynamic asset inventory and real-time monitoring of process data. Automatically establishes and maintains baseline configurations and inventory asset relationships, software, vendor references, firmware and hardware versions, serial numbers, PLC rack slot configuration, etc., throughout the environment. Information is shown in maps, tables, and reports that maintain an inventory of industrial assets, relationships, vulnerabilities, and programs they run. Includes behavioral analytics to detect process anomalies, faulty devices and unknown attacks to speed detection and prioritization of incident response. Includes threat intelligence from Cisco Talos and ICS CERT to help fix vulnerabilities, known and emerging threats.
FirePower Threat Defense combines next-generation firewall with next-generation intrusion prevention capabilities for essential cybersecurity controls for the systems and communication protection; detects potential cybersecurity events, IOCs; and identifies unauthorized protocols or software running on the network. Correlates vulnerability with threat information that delivers richer audit/log records for more efficient review and forensics analysis. Assists with the correlation of threats and actual asset vulnerability information to identify and document threats and calculate the impact assessment based on likelihood of attack success—essential to identify and prioritize responses based on risk and for immediate corrective actions. Also, provides visibility into software applications running on the network and builds/maintains accurate software application inventories.
TrustSec supports the IEEE 802.1X port-based access control using authentication and enables the network to function as an access policy enforcer through network segmentation more efficiently than internal firewalls, hard-to-manage ACLs, or legacy VLANs. Defines security requirements for systems communications at system boundaries, and supports forensic data gathering, storage, and transfer across systems. Enforces physical and logical access restrictions associated with changes to organizational systems. Helping to detect and report on events, TrustSec works with Cisco ISE to ensure only authorized individuals using authorized devices by enforcing the principles of least privileged secure access.
Umbrella DNS provides DNS layer security, secure web gateway (full proxy), and Cloud Access Security Broker (CASB) functionality in one platform. Verifies and controls/limits connections and information flows between security domains on connected systems. Logs and categorizes DNS activity for recall/deeper investigation. Exposes shadow IT by providing the ability to detect and report on the cloud applications in use. Provides ability to block specific user activities in select cloud apps. Integrates seamlessly with AnyConnect VPN.
Stealthwatch is an agentless solution that enables monitoring, logging, analysis, investigation and reporting of suspicious, unlawful and unauthorized system activity of users and devices by using telemetry from network infrastructure. Integrated with Cisco ISE, advanced threat detection, response and protection of critical data are enabled with smarter network segmentation. Stealthwatch is the only product that can detect malware in encrypted traffic and ensure policy compliance, without decryption.
AnyConnect VPN delivers scalable, secure remote access control that also provides context-aware, endpoint telemetry, comprehensive enforcement, unified endpoint posture checks, and automated remediation from any location, on any device, across wired, wireless, and VPN environments. Provides an IEEE 802.1X supplicant for Authentication, Authorization, and Accounting (AAA) capabilities. Monitors endpoint application usage to uncover potential behavior anomalies; usage data can be shared with NetFlow analysis tools such as Cisco Stealthwatch and Splunk to provide deep endpoint insight that even **EPP and EDR** solutions cannot address. Integrates effortlessly with ISE, Umbrella, and Duo MFA.

Advanced Malware Protection (AMP) uses global threat intelligence from Cisco's Talos to protect against known and emerging threats. Uses that intelligence and dynamic malware analysis technology to identify and block policy-violating file types, exploit attempts and malicious files trying to infiltrate the network. Continuously analyzes application data to understand threat and attack methods, detects malicious code on networks and endpoints (including mobile devices), assesses the potential impact, provides alerts and quarantines files. Provides file-and network-trajectory capabilities to analyze the effects and propagation of advanced malware-showing which systems were affected, and how deep the malware went into each system to understand the malware's impact and categorize the incident according to the response plan and perform the necessary forensics analysis to support response and recovery activities. Advanced sandboxing capabilities perform automated static and dynamic analysis of files against more than 700+ behavioral indicators. Cisco AMP for E-mail Security analyzes emails for threats such as zero-day exploits hidden in malicious attachments to provide advanced protection against spear phishing, ransomware, and other sophisticated attacks.
Tetration Platform processes comprehensive telemetry information of workloads—in the datacenter and cloud—received from software and hardware sensors in near-real time (up to 2 million events per second). Enforces consistent policy across thousands of applications running on tens of thousands of servers and can auto-generate granular application whitelist policies for segmentation across public and private clouds and on-prem. Applies advanced security analytics to speed event resolution, incident declaration, and root cause analysis. Designed with long-term data retention, searches tens of billions of telemetry records and returns actionable insights in less than a second. Also, checks if any of software packages have known information-security vulnerabilities listed in the **Common Vulnerabilities and Exposures (CVE)** database. When a vulnerability is detected, provides complete details, including the severity and the impact score, and locates all the servers that have the same version of the package installed; and, can execute predefined policies with specific actions, such as quarantining a host, when servers have packages with certain vulnerabilities.
Meraki appliances bring cloud-managed networking and unified threat management security to help small and medium-sized businesses and branch offices control network access, authenticate users and devices, secure their assets, data and users. Meraki enables administrators to automatically define security requirements for systems and communications, improve incident response, conduct configuration management activities, and implement/update system security plans at scale through the cloud.
Cisco Security Services helps integrate Cisco security technologies into multivendor environments; optimize your existing technologies to strengthen your security profile; and also support your migration from other solutions, including legacy products.

The bigger picture – securing the supply chain

The objective of the DoD's Cybersecurity Maturity Model Certification (CMMC) program is to implement **a new paradigm in security** designed to proactively enhance the aggregate protection of Controlled Unclassified Information (CUI) across the DIB. But, securing the DoD supply chain also encompasses additional necessary activities like those defined in Section 889(a)(1)(A) and (B) of the FY2019 NDAA which define certain banned products and technologies. Cisco's integrated security platform approach can automatically identify the use of covered telecommunications equipment or services in DIB enterprises or critical infrastructure systems spanning IT, OT, and IoT technologies.

Cisco Trustworthy Technologies provide a foundation of security and resilience across Cisco's solutions portfolio. Cisco Trustworthy Technologies provide product assurance functionality as well as foundational security capabilities which enhance the security and resilience of Cisco solutions. To protect against device counterfeiting and malicious attacks on hardware and software, Cisco uses digitally signed software images, hardware-anchored secure boot, Secure Unique Device Identifier (SUDI), and other trustworthy technologies to verify the authenticity and integrity of Cisco solutions. Among other functions, trustworthy technologies run automated checks of hardware and software integrity and can shut down the boot process if compromise is detected. Cisco Trust Anchor module provides a Secure Unique Device Identifier, highly secure storage, a random bit generator, and secure key management. These added layers of security protect against counterfeit and software modification; enable secure, encrypted communications; and verify that Cisco network devices are operating as intended.

Cisco Secure Development Lifecycle (SDL) is a repeatable and measurable process designed to increase Cisco product resiliency and trustworthiness. Cisco trustworthy security requirements focus on components such as credential and key management, cryptography standards, anti-spoofing capabilities, integrity and tamper protection, and session/data/ stream management. Also included is guidance for resilience and robustness, sensitive data disposal, and logging. This critical body of requirements is continually enhanced to incorporate new technologies and standards with the goal of building in inherent protections against evolving threats.

Cisco also strives to exceed industry standard security requirements (finance, medical, public utilities, and government). Therefore, Cisco is committed to government product certification processes and has a dedicated resource team for overall program management of global government certifications in support of building trustworthy products. Cisco maintains an active product certification and evaluation program for global government customers for certifications including: DoD Unified Capabilities Approved Products List (APL), Federal Information Processing Standard (FIPS 140), Federal Risk and Authorization Management Program (FedRAMP), Common Criteria, Internet Protocol v6, North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC-CIP), and others.

Finally, Cisco embeds multifaceted value chain security at every life cycle stage within its comprehensive Cisco cybersecurity strategy. Value chain security continually assesses, monitors, and improves the security of the third parties who are part of our solutions' life cycles. The scope of Cisco's commitment to security is unmatched in the industry.

Cisco's Layered Approach to Value Chain Security	Cisco Value Chain Security Process
• **Physical Security:** Practices including camera monitoring, security checkpoints, alarms and electronic or biometric access control. • **Logical Security:** Systematic, repeatable, and auditable operational security processes including encryption, materials and failure analysis segregation and scrap weight validation. • **Security Technology:** Technical innovation to enhance counterfeit detection, terminate functionality, or identify non-authorized components or users including smart chips, data-extracting test beds, and proprietary holographic or intaglio security labels. • **Information Security:** Data and information systems protection including remote access limitation, configuration management, network segmentation, multi-factor authentication and data classification.	**We manage a coordinated program across our engineering, manufacturing, and technical services teams, together with our global suppliers and channel partners to:** • Retain Cisco products and solutions in controlled development, manufacturing, logistics, and channel environments, using approved processes and tools, software and hardware components; • Prevent introduction of malware and/or rogue raw materials; • Develop technology, build devices, and deploy processes that make it more difficult to produce undetectable fake or altered Cisco solutions.

Cisco is committed to ongoing investment in innovation that enhances the security and resilience of our products and collaboratively driving enhanced security standards, policies, and tools across the global industry.

Simpler and more cost-effective security

With a Cisco Security Enterprise License Agreement, you can simplify the way you buy security products; help your company's resources go further; access new capabilities faster; and predictably spread costs over time. Legacy point-product security designs and ad hoc purchasing models and license tracking limits your operational efficiency and the effectiveness of the security systems you deploy. Cisco has simplified its licensing approach by offering Enterprise Agreements (EAs) to help you reduce costs and streamline license management under one platform. Cisco's approach of making software easier to buy, consume, and manage allows you to pick the right tool for the job without the delays and complexities that come with traditional licensing approaches.

Conclusion – A new paradigm to solve cybersecurity challenges

With the CMMC creating a **new paradigm** for ensuring robust cybersecurity practices from the Defense Industrial Base, **all suppliers** to the Federal Government and government agency executives should analyze their approach to integrated cybersecurity:

- Can you identify and apply micro-segmentation to every device on your network? Do you know if you have the correct policy controls for that device, and do you know if you can trust that device? Are you taking an approach that is founded in the principles of Zero Trust?
- Are you taking a "point solution-based" approach where your security team must integrate across disparately-related Network-Endpoint-Cloud siloed solutions that provide limited visibility and limited context across solutions – where your security teams have to be the integrator?
- Are you relying solely on a "technology based" approach that revolves solely around a single SIEM, SOAR, or equivalent, that requires complex integrations and lacks native controls and integrated policy management? Where your security teams still need to manually log into multiple appliances and systems to gather additional data when triaging events and simultaneously institute repetitive policies and controls?

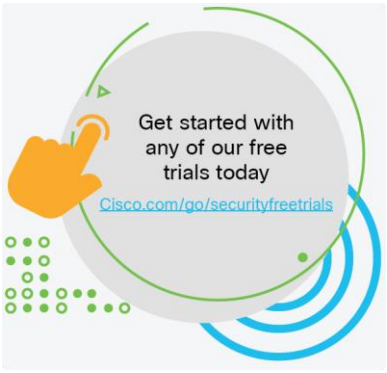
Rather, now it is time for a **new security paradigm with an integrated, portfolio-based platform**. One that security teams can easily integrate the products they use now, as well as cutting-edge products they'll want to use in the future to provide the most broad and consistent end-to- end coverage across all major threat vectors. There are a few differentiators to consider when evaluating your platform options and the portfolios they are built on:

Criteria	Look for
Protection	Broadly and globally deployed solutions that cover every threat vector and access point
Intelligence	A large threat research team that has a broad customer base for effective threat intelligence and analytics
Integration	A platform that offers out-of-the-box integration and openness at scale
Zero Trust	A platform and portfolio that offers a comprehensive approach to Zero Trust

Differentiators to consider when evaluating platform options

Additionally, consider the vendor's ecosystem of partners and third-party integrations. While the vendor's portfolio should provide a solid foundation for your platform, their partnerships, along with information exchange based on internet standards and well-documented APIs, will help you get the most out of your existing architecture.

Our goal is for you to be more secure and compliant—with less effort, less complexity, and greater visibility. **Protecting 100% of Fortune 100**, the industry-recognized leader in Zero Trust Security and Architecture, and leading solutions provider for the **DoD's Comply-to-Connect (C2C)** program, and the **Federal Government's Continuous Diagnostics and Mitigation (CDM)** program, Cisco delivers platform-level security and networking integrated solutions that span **IT, OT, campus, data center, network, cloud, internet, email, users, and everywhere in between**—built on **trustworthy technologies** and backed by Cisco Talos **threat intelligence** and vulnerability research teams—to help you protect the government's information and your company's enterprise from known APTs, zero-day attacks, malicious intent, and emerging threats.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C95-744153-00 08/20