



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

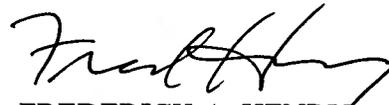
FEB 03 2014

DISA NOTICE 310-45-1-01*

ORGANIZATION

Single System Manager (SSM) for the Defense Switched Network (DSN)

- 1. Purpose.** This Notice identifies DISA Circular (DISAC) 310-45-1, Single System Manager (SSM) for the Defense Switched Network (DSN), as a legacy issuance.
- 2. Applicability.** This Notice applies to the Defense Information Systems Agency (DISA), the military departments (MILDEPs), and other Department of Defense (DoD) components and Government agencies including contractors.
- 3. Reference.** DISAN 210-20-02-01, DISA Issuances, 30 January 2014.
- 4. General.** Legacy circulars are for reference only and will not be updated. As a legacy circular, DISAC 310-45-1 is considered to be current in the DISA issuance postings and, accordingly, is exempt from a 5-year periodical review of content.
- 5. Justification.** The DSN voice services are evolving to DoD's Enterprise Voice over Internet Protocol (VoIP) communications services. The information contained in DISA Circular 310-45-1 is still valid and current until all DSN voice service is transitioned to VoIP.


FREDERICK A. HENRY
Brigadier General, USA
Chief of Staff

*This Notice will be canceled upon cancellation of DISA Circular 310-45-1 or be reissued within 5 years of its publication.

OPR: NS - disa.meade.ns.mbx.ns-front

DISTRIBUTION: P



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

DEC 6 2012

DISA CIRCULAR 310-45-1*

ORGANIZATION

Single System Manager (SSM) for the Defense Switched Network (DSN)

- 1. Purpose.** This Circular prescribes policy and describes organizational roles, responsibilities, and functions for the Single System Manager (SSM) for the Defense Switched Network (DSN). It also provides an overview of the communications relationships affecting the DSN SSM and describes the single system management of the DSN.
- 2. Applicability.** This Circular applies to the Defense Information Systems Agency (DISA), the military departments (MILDEPs), and other activities of the Department of Defense (DoD) and government agencies responsible for implementing procedures (implementers) and providing DSN services (providers) to authorized users.
- 3. Authority.** This Circular is published in accordance with the authority contained in DoD Directive 5105.19, Defense Information Systems Agency (DISA), 25 July 2006.
- 4. Policy.** This Circular is the governing directive for exercising single system management of the DSN.
- 5. Background.** A summary of the history and mission of DISA and an overview of the communications relationships affecting DISA as the DSN SSM are provided in enclosure 1.
- 6. Management.** The management of the DSN SSM is described in enclosure 2.
- 7. Responsibilities.** Organizational responsibilities for the DSN are detailed as follows. (A summarization of the Lead (L) and Support (S) responsibilities for various DSN-related activities is provided in enclosure 3.)

7.1 **Defense Information Systems Agency (DISA)**. The DISA SSM prescribes policy, provides procedures, assigns responsibilities, establishes technical requirements, monitors testing, and conducts certification and accreditation (C&A). The SSM also handles leases and procurements, installations, connections, and operations of telecommunications switches and services affecting the DSN. DISA will:

7.1.1 Act as DSN SSM by providing operational direction and management control of the DSN.

7.1.2 Chair and manage the *Voice Sensitive but Unclassified (SBU)* Configuration Control Board (CCB) and implement approved and funded Voice SBU CCB actions.

7.1.3 Manage the effectiveness of the DSN on a 24-hour-per-day, 7-day-per-week basis and evaluate operation and maintenance (O&M) practices and procedures ensuring command and control (C2) requirements are being met.

7.1.4 Report status and operational effectiveness of the DSN to the Joint Staff quarterly or more frequently if issues exist that may have a major effect on the network.

7.1.5 Recommend DSN performance objectives and establish interface criteria, in coordination with DoD components, and forward to the Joint Staff for approval.

7.1.6 Publish implementation documents for approved DSN objectives, in coordination with DoD components.

7.1.7 Review, process, and implement approved requests for DSN telecommunications service. (If any request for service has the potential to harm the network, DISA will forward the request to the Joint Staff for resolution regardless of designated approval level.)

7.1.8 Use exercises to verify readiness of the DSN and its ability to support user missions over the full range of stress scenarios.

7.1.9 Coordinate and assess funding amounts under the DISN Subscription Service (DSS) process.

7.1.10 Coordinate and review Command, MILDEP, and Agency policies and procedures on DSN use, where requested.

7.1.11 Review Command, MILDEP, and Agency DSN switch hardware and software, requests for proposals (RFPs), and contracts for compliance with configuration management (CM) and interoperability (IO) policy, where requested.

7.1.12 Process and implement approved DSN service agreements with foreign governments.

7.1.13 Provide technical evaluations for proposed schemes for automatic interconnection onto the DSN from public switched networks and forward a recommendation to the Joint Staff for approval or disapproval.

7.1.14 Implement network management procedures, *in coordination with the DISA Network Services Directorate (NS) Operational Support Systems Division (NS8)*.

7.1.15 Produce, update, and distribute the DSN Directory.

7.1.16 Recommend DSN consolidation and modification to improve network effectiveness or reduce costs.

7.1.17 Operate a DSN testing facility and maintain documentation pertaining to connection approval and interface standards. (The Joint Interoperability Test Command (JITC) will test or witness testing of all DSN components and interfaces before integration with the DSN; conduct developmental, operational, IO, environmental, and qualitative DSN testing; perform ongoing comprehensive evaluations throughout DSN program development; provide guidance to DSN users regarding test plans and conduct; certify tested entities for operation or IO with the DSN; document all test results and certifications; and provide lists of certified DSN components and configurations.)

7.1.18 Ensure only those switches and software loads that have been certified as interoperable by JITC and that have received security C&A are introduced into the DSN.

7.1.19 Disseminate specific instructions for operation of switching centers to the MILDEPs.

7.1.20 Maintain a database of all contractor DSN access requests, approvals, and terminations.

7.1.21 Implement controls necessary to limit DSN network access to those authorized by this Circular.

7.1.22 Provide an annual assessment of the impact of emerging voice processing and transport technology on global end-to-end voice performance and C2 services to the Joint Staff and the *Voice SBU* CCB.

7.1.23 Develop and maintain intraswitch and interswitch dialing plans to ensure standardization across the network.

7.2 **Combatant Commands.**

7.2.1 Define, validate, coordinate, and approve requirements for DSN service within their areas of purview.

7.2.2 Provide policy guidance and procedures in conformance with this Circular and in coordination with the MILDEPs and DISA for the use of the DSN within their respective areas of responsibility.

7.2.3 Provide acquisition, O&M, and logistics support for DSN customer premises equipment within facilities for which the combatant command is operationally responsible.

7.2.4 Coordinate with DISA before approval to determine if a DSN service request would degrade network performance.

7.2.5 Implement, control, and monitor use of precedence, on- and off-netting, and unofficial use of the DSN to prevent fraud, waste, or abuse.

7.2.6 Support DISA in contingencies, crises, and exercises involving operational elements of the DSN, as required.

7.2.7 Review and validate operational requirements for the DSN to meet requirements of operations, concept, and contingency and exercise plans.

7.2.8 Exercise review and approval authority over requirements for IMMEDIATE and PRIORITY precedence capability after DISA technically evaluates the request to determine potential network performance degradation and revalidate these requirements biennially.

7.2.9 Validate and forward requirements for FLASH and FLASH OVERRIDE to the Joint Staff for approval, in accordance with Chairman Joint Chiefs of Staff Instruction (CJCSI) *6211.02D, Defense Information Systems Network (DISN) Responsibilities.*

7.2.10 *Provide operational and performance metrics data to DISA as part of information sharing network management process.*

7.2.11 Provide copies of all contractor DSN access requests, approvals, and terminations to DISA.

7.2.12 Develop and implement policies and procedures to limit DSN use to that authorized by this Circular.

7.2.13 Coordinate all emerging technology base, post, camp, and station voice transport and processing initiatives with the DSN System Management Office (SMO).

7.3 Department of Defense (DoD) Components.

7.3.1 Define, validate, coordinate, and approve requirements for DSN services, in accordance with CJCSI *6211.02D*.

7.3.2 Participate in the Voice SBU CCB as a voting member.

7.3.3 Program, budget, acquire, operate, maintain, and fund assigned portions of the DSN for telecommunications services provided by the DSN and maintain switch hardware and software within three versions of the most current DISA IO certified and information assurance (IA) accredited release.

7.3.4 Register all DSN telecommunication switches and unified capabilities products that connect to the DSN-provided transport in the Systems Network Approval Process (SNAP) DSN module. (This includes unclassified voice, video, and data circuit registrations and connections and the upload of the DoD Information Assurance Certification and Accreditation Process (DIACAP) executive package artifacts in order to obtain connection approval in accordance with CJCSI 6211.02D.)

7.3.5 Validate and forward requirements for FLASH and FLASH OVERRIDE to the Joint Staff for approval, in accordance with CJCSI *6211.02D*.

7.3.6 Provide acquisition, O&M, logistics, and funding support for customer premises equipment and terminal equipment.

7.3.7 Provide training and periodic technical evaluations to ensure facilities, equipment, and personnel meet DSN performance objectives and interface requirements.

7.3.8 Provide policy, implement controls for, and monitor use of precedence, on- and off-netting, and unofficial use of the DSN to prevent fraud, waste, or abuse.

7.3.9 Support DISA during exercises involving operational elements of the DSN.

7.3.10 Review and validate operational requirements for DSN switches under their operational control.

7.3.11 Verify that only the new hardware and new software loads certified as interoperable and IA-accredited and placed on the Approved Products List (APL) by JITC are introduced into the DSN and verify that all older existing hardware and software in the end-to-end DSN global network will be IO-certified and IA-accredited upon upgrade, replacement, or relocation of equipment in support of new users.

7.3.12 Operate respective switching centers per directions disseminated by DISA.

7.3.13 Provide copies of all contractor DSN access requests, approvals, and terminations to DISA.

7.3.14 Develop and implement policies and procedures to limit DSN use to that authorized by this Circular.

7.3.15 Register all requirements for the DISN connection of emerging technology base, post, camp, or station voice systems using the SNAP, in accordance with CJCSI 6211.02D, and coordinate initiatives with the DSN System Manager (SM) for any new numbering requirements and transition to Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) transport.

7.3.16 Maintain DISA intraswitch and interswitch dialing plans for end users and implement the DSN access codes.

7.4 National Military Command System (NMCS) and the Joint Staff.

7.4.1 Define, validate, coordinate, and approve DSN telecommunications services requirements, in accordance with CJCSI 3170.01H, Joint Capabilities Integration and Development System.

7.4.2 Forward approved, planned DSN requirements and priorities for coordination and implementation.

7.4.3 Review and approve FLASH and FLASH OVERRIDE precedence calling requirements, as validated by the combatant commands, Services, and Agencies.

7.4.4 Ensure FLASH OVERRIDE and FLASH user missions continue to receive high precedence levels of service and initiate action to discontinue such access when mission needs change.

7.4.5 Review, validate, and approve DSN service requirements that might adversely affect the network but are required for mission accomplishment.

7.4.6 Review the operational effectiveness of the DSN. (Matters having a major effect on the network will be reported by the Joint Staff to the Office of the Secretary of Defense.

7.5 Non-Department of Defense (DoD) Agencies.

7.5.1 Define, validate, coordinate, and approve DSN requirements and priorities for telecommunications services.

7.5.2 Respond to DSN SSM guidance and direction.

7.5.3 Forward approved DSN requirements and priorities for coordination and implementation.

FOR THE DIRECTOR:

3 Enclosures a/s



FREDERICK A. HENRY
Brigadier General, USA
Chief of Staff

*This Circular cancels DISAC 310-45-1, 23 June 2008.

OPR: NS

DISTRIBUTION: P

Enclosure 1: DISAC 310-45-1

HISTORY AND MISSION OF DISA
AND COMMUNICATIONS RELATIONSHIPS AFFECTING THE
DEFENSE SWITCHED NETWORK (DSN) SINGLE SYSTEM MANAGER (SSM)

1. History and Mission of the Defense Information Systems Agency (DISA). The Defense Information Systems Agency (DISA) was established as a Department of Defense (DoD) agency in 1960. By authority of the Secretary of Defense, DoD Directive (DoDD) 5105.19, Defense Information Systems Agency (DISA), placed DISA under the direction, authority, and control of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO). The ASD(NII) was disestablished in January 2012, and the authorities, responsibilities, personnel, and resources of the ASD(NII) were transferred to the DoD CIO. The mission of DISA is described as being "responsible for planning, engineering, acquiring, testing, fielding, and supporting global net-centric information and communications solutions to serve the needs of the President, the Vice President, the Secretary of Defense, and the DoD Components, under all conditions of peace and war."

2. Communications Relationships Affecting the DSN SSM. The Defense Switched Network (DSN) is a worldwide network. For management purposes, it is subdivided into four major theaters of operation: Western Hemisphere, Europe, Pacific, and Central (Southwest Asia). The DSN is an interbase, nonsecure, and secure command and control (C2) telecommunications system for C2 and non-C2 authorized users in accordance with national security directives.

2.1 Global Information Grid (GIG). To accomplish its mission, DISA operates the Global Information Grid (GIG). The GIG is a globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policymakers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. It also includes National Security Systems (NSS), as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DoD, national security, and related intelligence community missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all

operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

2.2 Defense Information Systems Network (DISN). The Defense Information Systems Network (DISN) is the DoD global end-to-end information transfer infrastructure providing the communications infrastructure and services needed to satisfy national defense and command, control, communications, and intelligence (C3I) requirements and corporate defense requirements. The DISN includes the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet); the Secret Internet Protocol Router Network (SIPRNet); the Defense Red Switch Network (DRSN); the DSN; the DISN Video Services (DVS); Transport Services; and DISN Asynchronous Transfer Mode ATM Services (DATMS).

2.3 Defense Switched Network (DSN). The DSN is an interbase, nonsecure or secure DoD telecommunications system that provides dedicated telephone service, voice-band data, and dial-up video teleconference (VTC) for end-to-end command use and DoD authorized C2 and non-C2 users in accordance with national security directives. Nonsecure dial-up voice (telephone) service is the system's principal service. The Director, DISA, is the designated Single System Manager (SSM) for the DSN based on DoDD 5105.19 and accordingly *will "Perform systems engineering for the GIG to include the Defense Information Systems Network (DISN) to ensure that it is planned, operated, maintained, managed, and improved effectively and efficiently for end-to-end interoperability and mission capable architecture. The Director, DISA, shall exercise program management (with management control) over the activities of the DoD Components that directly support the DISN, and provide net-centric services and support for interagency, strategic, allied, multinational, coalition, joint, and combined command and control capabilities, in accordance with Presidential direction, memoranda of agreement, treaties, and international agreements." Management responsibility for both secure and nonsecure voice services has been further delegated to the Network Services Directorate (NS) Capabilities Center (NS2) Chief, Voice Services Division (NS22).*

2.3.1 The primary function of the DSN is to provide nonsecure voice (i.e., telephone and video conferencing) service. The DSN differs from all other circuit switched networks through the provisioning and utilization of military unique features (MUFs). A MUF consists of network and telecommunication switch features that are above and beyond those supported by commercial telephony carrier services to the general public. A MUF is intended to ensure the most critical calls receive preferential treatment

in terms of call completion. Specifically, the use of precedence and preemption classmarks ensure critical calls access hardware and software resources and supplant calls of less importance when required.

2.3.2 The DSN includes the end instruments; switches on the installations; backbone and tandem switches; transmission connectivity between and among the installations; Central Exchange (CENTREX) partitioned switches providing DSN service; network management system, timing and synchronization system; and signaling system. Voice processing and transport technologies (e.g., Voice over Internet Protocol [VoIP] or Voice over Asynchronous Transfer Mode [VoATM]) shall also be considered as elements of the DSN for meeting end-to-end performance requirements.

MANAGEMENT OF THE SINGLE SYSTEM MANAGER (SSM)
FOR THE DEFENSE SWITCHED NETWORK (DSN)

1. **General.** The Defense Switched Network (DSN) is unique among the Defense Information Systems Network (DISN) networks in that the assets which make up the network (switches) are owned, operated, and maintained by the military departments (MILDEPs). DISA provides the global oversight, guidance, network management system, and staffing down to the theater level as required to manage the DSN. Single system management is the process used by DISA, in collaboration with the MILDEPs, to manage the DSN over its entire life cycle. The process allows concurrent sustainment of the existing system, adaptation to changing requirements, and introduction of new procedures and technologies. The principal impetus for the process is to accomplish these activities while continually meeting performance metrics required by the Joint Requirements Oversight Council Memorandum (JROCM) 202-02, Global Information Grid (GIG) Mission Area Initial Capabilities.

1.1 In the role of the DSN Single System Manager (SSM), the Director, DISA, delegates authority to the DSN System Manager (SM) to implement appropriate policies and practices to manage the architecture, design, program planning, development, implementation, operation, interoperability (IO), and replacement of DSN elements to provide end-to-end command and control (C2) communications.

1.2 The DSN SM serves as the focal point for all DSN policies and procedures, working in conjunction with the Joint Staff, the combatant commands, and the DISN theater field offices. The DSN policies are issued to provide management guidance for the DSN. The DSN procedures are issued to provide the standardized methodologies required to implement the policies.

2. **Stakeholders.**

2.1 **Management Stakeholder.** DISA is the primary management stakeholder in the effective management of the DSN, and the Director, DISA, has delegated management authority for the DSN to the DSN SM.

2.2 **Operational Stakeholder.** The MILDEPs are the "operational" stakeholders and are tasked with responsibility for the procurement, installation, operation, and maintenance of individual DSN switches worldwide, in accordance with DSN SSM guidance.

The DoD components and contracted commercial telecommunications companies obtain and maintain interoperability and security of switches under their immediate control. *The MILDEPs ensure switches are operating in a manner that does not introduce vulnerabilities to the DSN and will operate and maintain their unclassified networks in accordance with all security policies, to include information assurance vulnerability management (IAVM) processes and all applicable Security Technical Implementation Guides (STIGs).*

2.3 Utilization Stakeholder. The DSN user community is the utilization stakeholder, depending on the network to provide all circuit-switched services required. Per Chairman, Joint Chiefs of Staff Instruction (CJCSI) *6211.02D, the DoD shall use the DISN-provided transport; i.e., the DSN. Use of non-DISN commercial transport as an alternative to DISN-provided transport requires a GIG waiver. DSN users must exercise telecommunications discipline utilizing the network for official use only; regulating use of military unique features (MUFs), such as multilevel precedence and preemption, only as needed; and reporting service issues through their appropriate reporting chain.*

3. Areas of Emphasis. The full spectrum of management issues is addressed by single system management across the life cycle of the network, to include development of policies and procedures, centrally managing numbering and routing, managing circuit provisioning, and many other disciplines. There are, however, specific management areas that receive particular attention.

3.1 Interoperability (IO) Certification and Information Assurance (IA) Accreditation. Any piece of equipment connected to the DSN must be both IO certified and IA accredited. As the DSN SSM, DISA develops processes, procedures, and technical standards that ensure DSN systems and components satisfy defined requirements for IO and supportability. Further, as the DSN SSM, DISA has overall responsibility for end-to-end operational integrity of the DSN. DISA develops procedures and technical standards to ensure DSN systems and components are tested to satisfy defined requirements for IA certification and accreditation (C&A). Connection to the DSN is approved by the *Network Services Directorate (NS) Enterprise Connection Division (NSC) for IO and IA certified equipment. In accordance with DoD Instruction (DoDI) 8100.04, DoD Unified Capabilities, only the DoD Chief Information Officer (DoD CIO) can approve IO and IA waivers or a request for an interim approval to operate (IATO).*

Requests for waivers or for an IATO shall be submitted via the Service or Agency chain of command to the DoD CIO stating the reason compliance is not possible.

3.2 Technology Migration. *As noted, the current Time Division Multiplex (TDM) technology base is being replaced by an Internet Protocol (IP) base. The transition to an IP-based system Sensitive But Unclassified (SBU) Voice will allow convergence of voice services into the overall unified capabilities and enterprise services schema. To ensure synchronization of efforts, all voice transport and processing initiatives shall be coordinated with the DSN SSM to coordinate access configurations and routing. The impact of emerging voice processing and transport technology on global end-to-end DSN performance and C2 services shall routinely be assessed by the DSN SSM.*

3.3 Network Performance Objectives (NPOs) and Voice Quality.

3.3.1 The NPOs are used to ensure quality of the voice networks and are intended to satisfy user requirements and reduce costs. The NPOs are recommended by DISA in coordination with the DoD components, validated by the Joint Staff, and approved by the DoD CIO. Commercial standards and practices are employed by the NPOs, when practical, to satisfy mission requirements. There are two general categories of NPOs--throughput and availability.

3.3.1.1 Throughput objective for routine precedence calls traversing the network is currently an intratheater grade of service (GoS) of P.07 (the probability of seven calls out of 100 being blocked during the busy hour expressed as a percentage) and an intertheater GoS of P.09 as measured during normal business hours of the theaters.

3.3.1.2 Network availability is a composite of switch availability and transmission availability. DISA, in conjunction with the operation and maintenance (O&M) commands, collects outage data across the network and compiles reports of network availability utilizing that data. An availability objective of 99.8 percent is the NPO.

3.3.2 While availability and throughput are all important factors, voice quality can be considered paramount. A connected call is of no use if the conversation between the two parties is unintelligible. Quality checks are performed on the current system, looking for echo and other factors that impact voice quality. With the pending conversion of current TDM voice

services to a converged IP-based packet network, new quality assurance (QA) checks are being implemented for factors such as latency.

4. **Annual Assessment.** An annual assessment on the impact of emergent voice processing and transport technology on global end-to-end voice performance and C2 services will be provided by the DSN SSM to the Joint Staff and the Voice SBU Configuration Control Board (CCB).

Enclosure 3: DISA CIRCULAR 310-45-1

DEFENSE SWITCHED NETWORK (DSN) RESPONSIBILITY MATRIX

RESPONSIBILITIES	DISA	COMBATANT COMMANDS	DOD COMPONENTS	NMCS AND JOINT STAFF	NON-DOD AGENCIES
Manage DSN contracts	L	S	S		
Manage DSS revenue	L	S	S	S	
Manage DSN program resources	L	S	S	S	
Oversee DSN operations	L	S	S	S	
Manage DSN revenue generation	L	S	S		
Develop and support DSN policy	L	S	S	S	
Approve requirements and priorities	S	L	S	S	
Approve requirements for telecomm services	S		L		
Approve requirements that might affect DSN	S		S	L	
Forward requirements to DISA	S	L	L	L	L
Provide combatant policy guidance	S	L	S	S	
Develop DSN concepts	L	S	S	S	S
Publish DSN Program Plan	L	S	S	S	S
Provide logistics planning and policy	S		L		L
Conduct switch inventory	S		L	S	L
Manage security	L	S	S	S	S
Manage connection approval process	L	S	S	S	S
Engineer developmental systems and components	L		S		S
Engineer operational systems and components	L		S		S
Provide technical assistance and insertion	L		S		S
Engineer system changes	L		S		S
Manage network configuration	L		S		S
Manage network implementation, transition, and execution	L		S		S
Manage interface development and implementation	L		S		S
Develop network system management (ADIMSS)	L		S		S
Implement topology and connectivity	L		S		S
Administer network O&M	L		S		S
Test and certify DSN and components	L	S	S		S
Provide operations direction and control	L		S	S	
Evaluate DSN O&M	L		S	S	
Support operations working groups	L	S	S	S	S
Review and approve Flash/Flash Override	S	S	S	L	
Change switch designation (i.e., MFS, EO, PBX)	S		S	L	

Legend: L - Lead Role (to guide the action); S - Support Role (to maintain the action)