DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, Maryland 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)
Office of Information Services (OIS)
Security and Standards Group (SSG)

CMS Information Systems Threat Identification Resource

Version 1.0
May 7, 2002

Table of Contents

1. Purpose

This threat identification resource has been developed to assist system owners and developers participating in the risk assessment process for the certification and accreditation of systems at the Centers for Medicare & Medicaid Services. This resource presents a broad view of the risk environment in which CMS operates today. The threats presented in this document were selected based on their occurrence and significance in the current CMS environment.

The resource has been divided into two sections. The first identifies threats that apply to Major Applications and Other Systems. The second addresses threats that are likely to affect General Support Systems.

Categories: The threat resource is categorized into four main groups: environmental/physical threats, human threats, natural threats, and technical threats. Those threats affecting Major Applications and Other Systems are divided into categories for human and technical threats. General support systems are subject to environmental/physical, human, natural, and technical threats. The categories list is not exhaustive. It was developed as a guide to spur identification of threats and vulnerabilities. As conditions and technology change, other categories not included here could apply to the system under review.

Threats: Within each section the threats are identified and described. The threat list is not exhaustive. Other threats not included here could apply to the system under review. For this reason, an entry for other threats has been included in each section. The effects of threats vary considerably from confidentiality and integrity of data to the availability of a system. Therefore, System Impact is identified within the threat column for each described threat.

Examples: To further assist those consulting this resource, examples of each type of threat have been provided. The examples are not all inclusive. They provide guidance. Other conditions requiring consideration may be present for the system under consideration. If they exist, these conditions should be addressed by system owners and developers.

2. Threats to MA and Other Systems

This section addresses threats to MAs and Other Systems with descriptions and examples. Threats to these systems may stem from human and technical sources.

2.1 Human Threats to MAs and Other Systems

HUMAN THREATS (MA)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
1. Data Entry Errors or Omissions ***System Impact*** *Could significantly impact data integrity, and to a lesser extent data availability.*	Data entry errors and omissions are mistakes in keying or oversight to key data, which could affect system resources and the safeguards that are protecting other system resources.	• Failure to disable or delete unnecessary accounts, such as guest accounts and employees that no longer need access to system resources could result in unauthorized access to sensitive data. • Entering incorrect values for sensitive information such as SSN, financial data or personally identifiable data could result in data inconsistency. • Innocent data entry errors could result in inconsistency in spellings, which could make accurate reporting, or standard searches impossible.
2. Inadvertent Acts or Carelessness ***System Impact*** *Could significantly impact data confidentiality, integrity, and availability.*	Inadvertent acts or carelessness are unintentional acts that could cause system performance degradation or system loss.	• Programming and development errors result in software vulnerabilities. Successful compromise could lead to loss of data confidentiality, integrity, and availability. • Incorrect operations of database synchronization procedures could result in data errors, including entry, deletion, and corruption errors. • Improper upgrades to database management software could result in vulnerabilities that could impact data confidentiality, integrity, and availability.
3. Impersonation ***System Impact*** *Could significantly impact data confidentiality, and to a lesser extent data integrity and availability.*	Impersonations are threats that often become enablers for other threats. Impersonation for physical access could include misuse of badges, key cards, personal Identification numbers (PIN), etc. Impersonation for electronic or system access could include use of others' identification and authentication	• Sharing of badges, key cards, and PINs could provide an employee or cardholder with unauthorized access to sensitive information. • Forged documents could form the basis for data entry, modification, or deletion. • Social engineering such as tricking employees into revealing passwords or other information can compromise a target system's security.

HUMAN THREATS (MA)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
	information in an attempt to gain system privileges and access to system resources.	
4. Shoulder Surfing ***System Impact*** *Primarily impacts data confidentiality, but in combination with other threats could impact integrity and availability.*	Shoulder Surfing is the deliberate attempt to gain knowledge of protected information from observation. The unauthorized disclosure of protected information leads to information misuse (identity theft), or such information could be used to gain additional access or information.	• Housekeeping staff could observe the entry of sensitive information. • Failure to protect a UserID and Password from observation by others during logon could allow unauthorized users to capture sensitive information. • Visitors could capture employee's passwords and other sensitive information left unprotected on desktops.
5. User Abuse or Fraud ***System Impact*** *Could significantly impact data confidentiality, integrity, and availability.*	User abuse or Fraud addresses authorized users who abuse their assigned access privileges or rights to gain additional information or privileges.	• Users could browse systems and applications in search of specific data or characteristics. • Use of information (password) as an indirect aid for subsequent misuse, including unauthorized access could compromise data security. • Information (Social Security numbers) could be used as a direct aid for illegal purposes, including identity theft.
6. Theft, Sabotage, Vandalism, or Physical Intrusions ***System Impact*** *Could significantly impact data integrity and availability, and to a lesser extent data confidentiality.*	Theft, sabotage, vandalism, or physical intrusions are deliberate malicious acts that could cause damage, destruction, or loss of system assets. Such an act could	• Disgruntled employees could create both mischief and sabotage of system data. • Deletion or corruption of data could occur through acts of vandalism. • Logic bombs could destroy system data at a given time or under certain circumstances. • Sensitive data could be captured through application vulnerabilities, and held hostage. • Cleaning staffs/vendors could have access

HUMAN THREATS (MA)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
	also enable other threats, such as compromise of interconnected systems.	to sensitive information.
7. Espionage ***System Impact*** *Significantly impacts data confidentiality, but combined with other threats could impact data integrity and availability.*	Espionage is the covert act of spying through copying, reproducing, recording, photographing, interception, etc., to obtain information.	• Espionage could be conducted by foreign governments through technical means, such as electronic bugs and wire taps. • Foreign government could recruit an agent inside the target agency by either bribing or blackmailing an employee. • Medical companies could encourage employees to take positions in CMS to provide them with a constant supply of information. • The use of legitimate business agreements, such as licensing and on-site liaison officers or contractors, could be used to provide unauthorized opportunities to gather information.
8. Other Threats…	(To be specified by system owner or developer.)	

2.2 Technical Threats to MAs and Other Systems

TECHNICAL THREATS (MA)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
1. Misrepresentation of Identity ***System Impact*** *Could significantly impact data confidentiality, and to a lesser extent data integrity and availability.*	Misrepresentations of identity are threats that often become enablers for other threats. Misrepresentation for electronic or system access could include use of others' identification and authentication information in an attempt to gain privileges into	• Abuse of privileges such as misuse of USERIDs and passwords could be used to gain unauthorized access to sensitive data. • Personal profile extraction could allow an unauthorized person to assume an otherwise authorized role. • Forged documents and messages could form the basis for costly business decisions. • Social engineering, such as tricking employees into revealing passwords or other information that provides access to an application could compromise data security.

TECHNICAL THREATS (MA)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
	system resources.	
2. Intrusion or Unauthorized Access to System Resources ***System Impact*** *Could significantly impact data confidentiality, integrity, and availability.*	Intrusion or Unauthorized Access to System Resources is gaining unauthorized access to system resources. The intent could be malicious or non-malicious (e.g., curiosity seeker) in nature.	• Trojan Horses perform malicious system actions in a hidden manner, including file modification, deletion, copying, or the installation of system backdoors. Some examples are SubSeven Trojan, NetBus, BackOrifice, and Deep Throat. • Trap Door (back door) attacks could result in improper identification and authentication, improper initialization or allocation, improper runtime validation or improper encapsulation.
3. Data/System Contamination ***System Impact*** *Could significantly impact data confidentiality, and to a lesser extent data integrity and availability.*	Data/system contamination is the intermixing of data of different sensitivity levels, which could lead to an accidental or intentional violation of data integrity.	Data values that stray from their field descriptions and business rules could be revealed to unauthorized persons. • Anomalies and multiple account numbers for the same entity could allow unauthorized access to data. • Corrupted system files could contain strings of sensitive information. • File fragments containing sensitive information could be scattered throughout a drive instead of in an encrypted sector to protect them from compromise. • Cross-site scripting attacks (CSS) could be launched by inserting malicious tagging as an input into dynamically generated web pages. Malicious tagging could enable an attacker to accomplish compromise of data integrity, set and read cookies, intercept user input and execute malicious scripts by the client in the context of the trusted source. For example, Citibank closed a CSS vulnerability identified by De Vitry at the bank's C2IT.com Internet payment site that enabled attackers to grab users' credit card and bank account information.
4. Eavesdropping ***System Impact*** *Could significantly impact data*	Eavesdropping is the deliberate attempt to gain knowledge of protected	• Eavesdropping devices, such as Electronic Bugs, could be used to intercept sensitive, unencrypted data. For example, Keystroke monitoring could transmit every keystroke so that all user input could be reproduced.

TECHNICAL THREATS (MA)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
confidentiality, but combined with other threats could impact data integrity and availability as well.	information. The unauthorized disclosure of protected information leads to information misuse (identity theft), or such information could be used to gain additional access or information.	• Trojan Horse applications could surreptitiously capture user or system activities.
5. Insertion of Malicious Code or Software; or Unauthorized Modification of a Database. ***System Impact*** *Could significantly impact data confidentiality, integrity, and availability.*	Insertion of Malicious Code or Software; or Unauthorized Modification of a Database is the malicious intent to change a system's configuration without authorization by the addition or modification of code, software, database records, or information. The intent and impact could range from subtle annoyances and inconveniences to catastrophic failures and outages.	• Modification, insertion, or deletion of data or lines of code could compromise data and/or system. • Unauthorized modification of database records could compromise data integrity and availability. • Trojan Horse applications could be installed through code and software modifications. Some examples are SubSeven Trojan, NetBus, BackOrifice, NetCat and Deep Throat • Logic bombs could be placed within authorized software and perform malicious system actions on a given trigger event. • Trap door functions could be inserted into authorized code and software. • Improper database entries and updates could be executed.
6. Takeover of Authorized Session ***System Impact*** *Could significantly impact data confidentiality, and to a lesser extent data*	Takeover of Authorized Session is gaining control of an authorized session, and assuming the access rights of the authorized party.	• Network sessions could be compromised through session hijacking techniques. • When a user leaves the immediate work area and a session remains open, unauthorized use could occur. • Database communications could be captured, modified, and sent to the original destination.

TECHNICAL THREATS (MA)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
integrity and availability.	This session could be used for further unauthorized access.	
7. System and Application Errors, Failures, and Intrusions not Properly Audited and Logged ***System Impact*** *Could significantly impact data integrity and availability.*	Auditing and logging of system and application errors enable administrators to troubleshoot and safeguard performance issues, and reconstruct events of unauthorized access. The lack of sufficient auditing and logging of System and Application Errors, Failures, and Intrusions reduces these capabilities.	• Auditing and logging settings not properly configured at the system and application level could prevent tracking of malicious acts. • Intruders could gain unauthorized system access and abort auditing processes. • If Audit logs reach their maximum threshold they could remove logged data, or stop logging new data.
8. Other Threats…	(To be specified by system owner or developer)	

3. Threats to GSS

This section addresses threats to GSSs with descriptions and examples. Threats to these systems may stem from environmental/physical, human, natural and technical sources.

3.1 Environmental and Physical Threats to GSSs

ENVIRONMENTAL/PHYSICAL THREATS (GSS)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
1. Environmental Conditions ***System Impact*** Primarily affects the integrity and *availability of the system*.	Environmental conditions are controlled and non-controlled climate conditions, which have the potential to cause system damage or	• Water leaks in server rooms could cause equipment damage. • Both excess and insufficient humidity in the computer room could threaten system reliability. • Overheating in computer rooms could result in computer failure and downtime.

ENVIRONMENTAL/PHYSICAL THREATS (GSS)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
	degradation. This threat could be a result of the natural environment (extreme heat, cold, humidity, etc.) or faulty/poorly designed heating, ventilation, and air conditioning systems.	• Poor ventilation and air conditioning failure in server rooms could cause mechanical parts, such as disk drives containing data, to fail. • Air conditioning system failure could impair utilization of the building due to excessive heating, cooling, or insufficient air exchange.
2. Electromagnetic Interference (EMI) ***System Impact*** *Primarily affects the integrity and availability of the system.*	Electromagnetic Interference (EMI) is the impact of signal transmitters and receivers operating in proximity to a CMS system, which could cause an interruption in the electronic operation of the system.	• Malfunctioning equipment: Electromagnetic impulses and radio frequency interference (RFI) are common causes of line noise. Line noise could cause corrupted data transfers from a CPU to disk, printing errors, power supply damage, and static on computer monitor screens. • EMI could cause an extended power surge, over-stress power supplies and lead to computer equipment damage. • EMI could cause a power failure, disrupting network operation, computer screens to go blank, and servers to crash. • Electromagnetic radiation from standard computers could be used to reconstruct the contents of the computer screen. These signals could carry a distance of several hundred feet, and even further if exposed cables or telephone lines act as unintended antennas.
2. Electromagnetic Interference (EMI) ***System Impact*** *Primarily affects the integrity and availability of the system.*	Electromagnetic Interference (EMI) is the impact of signal transmitters and receivers operating in proximity to a CMS system, which could cause an interruption in the electronic	• Malfunctioning equipment: Electromagnetic impulses and radio frequency interference (RFI) are common causes of line noise. Line noise could cause corrupted data transfers from a CPU to disk, printing errors, power supply damage, and static on computer monitor screens. • EMI could cause an extended power surge, over-stress power supplies and lead to computer equipment damage..

ENVIRONMENTAL/PHYSICAL THREATS (GSS)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
	operation of the system.	• EMI could cause a power failure, disrupting network operation, computer screens to go blank, and servers to crash. • Electromagnetic radiation from standard computers could be used to reconstruct the contents of the computer screen. These signals could carry a distance of several hundred feet, and even further if exposed cables or telephone lines act as unintended antennas.
3. Hazardous Material Accident ***System Impact*** *Could impact system availability.*	Hazardous material accident is the unexpected spill of toxic material. Hazardous materials are substances that are either flammable, oxidizable or combustible, explosive, toxic, noxious, corrosive, an irritant or radioactive.	• Office cleaning materials with flammable contents could cause a fire or explosion if spilled or not kept at a specific temperature. • Spilled chemicals could cause a fire, releasing toxic smoke. • Chemical drain cleaners (also called drain openers) are extremely corrosive. Common ingredients in drain cleaners include lye or sulfuric acid. These chemicals work by eating away materials including skin if they should come in contact. • Household ammonia is considered to be an irritant rather than a corrosive hazard. Vapors, even in low concentrations, can cause severe eye, lung, and skin irritation. Chronic irritation may occur if ammonia is used over long periods of time. • Solvents such as alcohols are considered combustible because they evaporate easily at room temperature and can readily ignite given heat, spark, or flame. • Bleach, when mixed with phosphoric acid cleaner, produces a noxious gas with a strong odor.
4. Physical Cable Cuts ***System Impact*** *Could affect system availability.*	A physical cable cut could be an intentional or unintentional event that affects the system's ability to perform its intended	• A disgruntled employee could sabotage transmission media • Animals could cause damages to cables resulting in broken cables. • Lightening strikes could cause a structural fire, which could, in turn, burn out circuits resulting in a power failure.

ENVIRONMENTAL/PHYSICAL THREATS (GSS)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
	function. Depending upon the power and communications backups built into the system, the effects could range from minimal to catastrophic.	• Lightening strikes could cause a structural fire, which could, in turn, burn out circuits resulting in a power failure. • Lightening strikes could cause severe damage resulting in broken cables.
5. Power Fluctuation ***System Impact*** *Could impact system availability.*	Power Fluctuation is a disruption in the primary power source (power spike, surge, brownout, and blackout) that results in either insufficient or excessive power.	• A power outage could affect the timeliness and quality of the delivered service. • Malfunction or failure of Central Processing Unit (CPU) or hardware could impact the timeliness and quality of the delivered services.
6. Secondary Disasters ***System Impact*** *Could affect system availability.*	Secondary disasters are successive disasters that are likely to result from natural disasters or environmental conditions. Secondary disasters could strike communities at any time, with or without warning. The probability of secondary disasters should be anticipated.	• Spilled chemicals could cause a fire, releasing toxic smoke. • Broken water pipes could cause internal flooding. • An earthquake could cause a structural fire, which could, in turn, burn out circuits resulting in a power failure.
7. **Other Threats**	(To be specified by system owner or developer)	

3.2 Human Threats to GSSs

HUMAN THREATS (GSS)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
1. Arson ***System Impact***	Arson is the willful and generally malicious burning or starting of fires	• Malicious fires caused by bombs and incendiary devices could result in damage or destruction of system hardware and loss of data

HUMAN THREATS (GSS)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
Primarily affects system availability.	starting of fires.	of data. • The malicious intent could be the cause of a fire resulting from a contact of steel wool cleaning material and metal or wiring.
2. Improper Disposal of Sensitive Media ***System Impact*** Primarily affects confidentiality, but in combination with other threats could impact integrity and availability.	Improper Disposal of Sensitive Media is the discarding of information improperly which could result in compromise of sensitive information.	• Searching for residual data left in a computer, computer tapes, and disks after job execution could compromise that data. • Disposing of previously owned client PCs that contain sensitive and unclassified information could reveal sensitive data. • Readable data can be retrieved from hard copies, wastepaper baskets, magnetic tapes, or discarded files resulting in compromise of that data.
3. Shoulder Surfing ***System Impact*** *Primarily affects confidentiality, but in combination with other threats could also affect integrity and availability.*	Shoulder surfing is the deliberate attempt to gain protected information. The unauthorized disclosure of protected information leads to information misuse.	• Allowing remote dial-up access to networks or systems from off-site locations could disclose an agency's dial-up access phone number, user account, password, or log-on procedures. • Personal standalone workstations could be unprotected. • Visitors could capture employee's passwords and other sensitive information.
4. Inadvertent Acts or Carelessness ***System Impact*** *Could impact confidentiality, integrity, and availability.*	Inadvertent acts or carelessness are unintentional acts that could cause system performance degradation or system loss.	• Programming and development errors could cause a buffer overflow. This leaves the system exposed to security vulnerabilities. • Installation, upgrade and maintenance errors could leave data unprotected or overly exposed to security vulnerabilities. • Failure to disable or delete unnecessary accounts (network, Internet, and voice), such as guest accounts, and terminated employees could result in unauthorized access to sensitive data. • Failure to recover terminated employees' card keys and door keys could provide unauthorized access to system and data.

HUMAN THREATS (GSS)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
5. Omissions ***System Impact*** *Primarily affects the confidentiality, integrity and availability of the system.*	Omissions are non-malicious threats that could affect system resources and the safeguards that are protecting other system resources.	• Failure to disable or delete unnecessary accounts (network, Internet, and voice), such as guest accounts and employees that no longer need access could provide unauthorized access to system resources. • Failure to recover terminated employees' card keys and door keys could provide unauthorized access. • If the system administrator fails to perform some function essential to security, it could place a system and its data at risk of compromise.
6. Procedural Violation ***System Impact*** *Primarily affects availability of the system.*	Procedural violation is the act of not following standard instructions or procedures, which could be either intentional or unintentional.	• Refusal to carry out work related instructions or tasks, such as the refusal to remove a User ID and logon access of an employee terminated for cause could place a system and data at risk of compromise. • Unintentional failure to carry out work-related instructions or tasks, such as the failure to test a backup tape to determine whether or not the backup was successful could place data at risk of loss.
7. Scavenging ***System Impact*** *Primarily affects confidentiality.*	Scavenging is the searching through object residue to acquire sensitive data.	• Searching for residual data left in a computer, computer tapes, and disks after job execution could compromise that data. • Examining discarded or stolen media could reveal sensitive data.
8. Theft, Sabotage, Vandalism, or Physical Intrusions ***System Impact*** *Could impact confidentiality, integrity, and availability of the system.*	Theft, sabotage, vandalism, or physical intrusions are deliberate malicious acts that could cause damage, destruction, or loss of system assets. Such an act could also enable other threats, as in the sabotage of a system to gain access to and compromise other interconnected CMS systems.	• Disgruntled employees could sabotage a computer system by installation of software that could damage the system or the data. • Destruction of hardware or facilities could destroy data that might not be recovered. • Computer abuse such as intentional and improper use, alteration and disruption could result in loss of system assets. • Cleaning staffs/vendors or contractors could steal unsecured sensitive information.

HUMAN THREATS (GSS)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
9. User Abuse ***System Impact*** *Could impact confidentiality, integrity, and availability of the system.*	User abuse addresses authorized users who abuse assigned access privileges or rights, to gain unauthorized access to information or privileges.	• A user could engage in excessive use of an Information System asset for personal means (e.g., games, resumes, personal matters). • A user could search through electronic storage to locate or acquire information. • A user could browse randomly or search for specific characteristics. • The opening of an unprotected port on a firewall could provide unauthorized access to information.
10. Espionage ***System Impact*** *Espionage could primarily impact confidentiality and availability.*	Espionage is the covert act of spying through copying, reproducing, recording, photographing, interception, etc., to obtain information.	• Espionage could be conducted by foreign governments through technical means, such as electronic bugs and wire taps. • A foreign government could recruit an agent inside the target agency by either bribing or blackmailing an employee. • Companies could encourage employees to take positions in CMS to provide those companies with a constant supply of information. • Legitimate business agreements, such as licensing and on-site liaison officers or contractors could be used to provide unauthorized opportunities to gather information.
11. Labor Unrest ***System Impact*** *Primarily affects the availability of the system. Could also affect confidentiality and integrity.*	Labor unrest is activities organized by employees designed to halt or disrupt normal operations such as strike, walkout, and protest job action.	• The unavailability of key personnel resources could disrupt normal operations. • Employee refusals to carry out work-related instructions or tasks could pose a threat to information security if they refuse to close vulnerability.
12. Terrorism ***System Impact*** *Primarily affects confidentiality, integrity and availability.*	Terrorism is a deliberate and violent act taken by an individual or group whose motives go beyond the act of sabotage, generally toward some extreme	Terrorism is a constant danger as illustrated by the following attacks: • September 11, 2001 attacks. • Bomb threats/attempts e.g. 1998 Embassy bombings, 1993 World Trade Center Bombing. • Biological attack e.g. post September 11, 2001 anthrax attack. • Cyber terrorism or information warfare. For

HUMAN THREATS (GSS)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
	political or social sentiment.	example, Hackers broke into the U.S. Justice Department's web site and replaced the department's seal with a swastika, redubbed the agency the "United States Department of Injustice" and filled the page with obscene pictures. Also, in December 2001, computer hackers tapped into WebCom, one of the nation's largest worldwide web service providers on the Internet, and removed more than 3,000 sites for 40 hours, many of them retailers trying to capitalize on the Christmas rush.
13. Riot/Civil Disorder ***System Impact*** *Primarily affects the availability of the system.*	Riot/civil is a violent disturbance created by and involving a large number of people, often for a common purpose or over a significant event.	• The unavailability of key personnel resources could affect system availability. • The refusal to carry out work-related instructions or tasks could affect data availability. • Employees might not be able to reach the workplace to ensure data protection.
14. Other Threats	(To be specified by system owner or developer)	

3.3 Natural Threats to GSSs

NATURAL THREATS (GSS)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
1. Natural Disaster ***System Impact*** *Could impact system availability.*	Natural disasters, such as hurricanes, wind damage/tornadoes, earthquakes, and floods could result in damage or destruction of system hardware or software assets. Any of these potential threats could lead to a partial or total outage.	• An internal/external fire could result in damage to system hardware and facility. • Internal/external flooding could result in damage or destruction of system hardware. • Earthquakes are among the most deadly and destructive of natural hazards. They could be the direct cause of injury or death to a person responsible for security. They often destroy power and telephone lines. They could cause severe damage to facilities.

NATURAL THREATS (GSS)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
2. Secondary Disaster ***System Impact*** *Primarily affects the availability of the system.*	Secondary disasters are successive disasters that are likely to result from natural disasters or environmental conditions. Secondary disasters could strike communities at any time, with or without warning. The probability of secondary disasters should be anticipated.	• An earthquake could cause a structural fire, which, in turn, could burn out circuits resulting in a power failure. • Intense rains could cause flooding. • Spilled chemicals could cause a fire. • Broken water pipe could result in internal flooding.
3. Other Threats	(To be specified by system owner or developer)	

3.4 Technical Threats to GSSs

TECHNICAL THREATS (GSS)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
1. Data/System Contamination ***System Impact*** *Primarily affects the confidentiality, integrity, and availability of data.*	Data/system contamination is the intermixing of data of different sensitivity levels, which could lead to an accidental or intentional violation of data integrity.	• Data values that stray from their field descriptions and business rules could be revealed to unauthorized person. • Anomalies and multiple account numbers for the same entity could allow unauthorized access to data. • Cross-site scripting attacks (CSS) could be launched by inserting malicious tagging as an input into dynamically generated web pages. Malicious tagging could enable an attacker to accomplish compromise of data integrity, set and read cookies, intercept user input and execute malicious scripts by the client in the context of the trusted source. For example, Citibank closed a CSS vulnerability identified by De Vitry at the bank's C2IT.com Internet payment site that enabled attackers to grab users' credit card and bank account information.
2. Compromising	Compromising	• Radiation or signals that emanate from a

TECHNICAL THREATS (GSS)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
Emanations ***System Impact*** *Primarily affects confidentiality.*	Emanations is the unintentional data-related or intelligence-bearing signals, which, if intercepted and analyzed, could disclose sensitive information being transmitted and/or processed by the CMS system.	communications circuit could disclose to unauthorized persons or equipment the sensitive or proprietary information that is being transmitted via the circuit. • Use of an inductive amplifier on unprotected cable could reveal unencrypted data and passwords.
3. Corruption by System, System Errors, or Failures ***System Impact*** *Could impact confidentiality, integrity, and availability of the system.*	Corruption by System, System Errors, or Failures addresses corruption of a system by another system, system errors that corrupt data, or system failures that affect system operation.	• Failure of system software/hardware could result in database failures leading to financial loss. • Failure of application software could prevent users of these applications from performing some or all of the tasks assigned to them unless these tasks could be carried out manually. • Flawed designs, such as newly discovered vulnerabilities not addressed by requirements could place system at risk of compromise. • Faulty implementation, such as inconsistency with design or new bugs not covered by specifications could allow compromise of data and application.
4. Eavesdropping ***System Impact*** *Could impact confidentiality, but in combination with other threats could impact integrity and availability.*	Eavesdropping is the deliberate attempt to gain protected information. The unauthorized disclosure of protected information leads to information misuse (identity theft), or it could be used to gain additional access or information.	• Eavesdropping devices, such as Electronic Bugs could capture system activity. • Keystroke monitoring could transmit every keystroke so that all user input could be reproduced. • Use of an inductive amplifier on unprotected cable could permit unauthorized intercept of transmission. These transmissions could include sensitive information, such as passwords, in the clear. • Use of a Packet Sniffers could permit unauthorized intercept of transmission. These transmissions could include sensitive information, such as passwords over networks (e.g., in telnet or ftp). • Electromagnetic radiation from standard

TECHNICAL THREATS (GSS)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
		computers could be used to reconstruct the contents of the computer screen. These signals could carry a distance of several hundred feet, and even further when exposed cables or telephone lines function as unintended antennas. • Attackers could use offshore hackers to break into Federal computer systems and steal protected information. The fact that the attack could come from outside the United States increases the difficulty of protection.
5. Misuse of Known Software Weaknesses ***System Impact*** *Could impact confidentiality, integrity and availability.*	Misuse of Known Software Weaknesses is the deliberate act of bypassing security controls for the purpose of gaining additional information or privileges. This weakness could be at the operating system, application or access control levels of a system.	• User IDs, especially root/administrator with no passwords or weak passwords for all systems could allow unauthorized access to the application and its data. • Remote Procedure Call (RPC) weaknesses in rpc.ttdbserverd (ToolTalk), rpc.cmsd (Calendar Manager), and rpc.statd could allow root compromise. This affects multiple Unix and Linux systems. • IMAP and POP buffer overflow vulnerabilities or incorrect configuration could allow compromise of data and application. • Sendmail buffer overflow weakness, pipe attacks and MIMEbo could allow compromise at the root level. • Global file sharing and inappropriate information sharing via NFS and Windows NT ports 135-139 (445 in windows 2000) or UNIX NFS exports on port 2049 as well as Appletalk over IP with Macintosh file sharing enabled, could result in data compromise. • The RDS security hole in the Microsoft Internet Information Server (IIS) could allow an attack to damage or destroy the application and its data.

TECHNICAL THREATS (GSS)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
6. Hardware / Equipment Failure ***System Impact*** *Primarily affects the integrity and availability of the system.*	Hardware / Equipment Failure is the unexpected loss of operational functionality of any CMS system hardware asset.	• Malfunction or failure of Central Processing Unit (CPU) or other hardware could result in the loss of system data. • Faulty network components such as hosts, routers and firewalls could result in interruption of communications between the connected stations. • Improper hardware maintenance could allow a system crash to occur. • Internal power disturbances could result in loss of system data. • Self-generated or other internal interference could damage data or interrupt system function.
7. Insertion of Malicious Code, Software, or Database Modification ***System Impact*** *Could impact confidentiality, integrity and availability.*	Insertion of Malicious Code, Software, or Database Modification is the malicious intent to change a system's configuration by the addition or modification of code, software, hardware, database, or information, without authorization. The intent and impact could range from subtle annoyances to severe failures and outages.	• Introduction of network worms, such as Code Red worm, W32/Leaves worm, and power worm could damage the system and associated data. • Modification, insertion, or deletion of lines of code, software, hardware and database could result in system malfunction and loss of system data. • Trojan Horse applications could be inserted into authorized software. Some examples are SubSeven Trojan, Barok, Kuang2 pSender Full, Sesame, and Deep Throat. This could result in system damage and data compromise. • Virus code, such as W97M.Mailissa, Merry XMAS or Independence Day, could be inserted into authorized software resulting in system damage and data compromise. • Denial of Service (DOS) and Distributed Denial of service (DDOS) attacks such as worms could execute Network saturation attacks or bandwidth consumption attacks interrupting system access. • Improper database updates could result in data damage or loss.
8. Installation Errors ***System Impact***	Installation errors are the errors, which could occur as a of result poor	• Poor installation procedures could leave data unprotected, e.g. built-in security features of software packages are not implemented. • Failure to educate and prepare for installation

TECHNICAL THREATS (GSS)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
Could impact confidentiality, integrity and availability of the system.	installation procedures. Installation errors whether hardware or software, could undermine security controls.	and uninstallation methods could leave data unprotected. • Incorrect installation or a conflict with another device that is competing for the same resources within the computer system could impact system data and resource availability. • Installation of programs designed by users for personal computers could modify the system initialization scripts and change the configuration of a system allowing unauthorized access to sensitive data. • Installation of patches and hot fixes could modify the system initialization scripts and change the configuration of a system. This could reset security settings and place data at risk of compromise.
9. Intrusion or Unauthorized Access to System Resources ***System Impact*** *Depending on the level of intrusion and the safeguards, the intrusion or unauthorized access to system resources could impact confidentiality, integrity, and availability.*	Intrusion or Unauthorized Access to System Resources is gaining unauthorized access to system resources. The intent could be malicious or non-malicious (e.g., curiosity seeker) in nature.	• Trojan programs perform malicious system actions in a hidden manner, including file modification, deletion, and copying, or the installation of system backdoors. Some examples are SubSeven Trojan, Barok, Kuang2 pSender Full, Sesame, and Deep Throat. • Network worms, e.g. Code Red worm, W32/Leaves worm, and power worm could damage the system and associated data. • Trap Door (back door) attacks could result in improper identification and authentication, improper initialization or allocation, improper runtime validation and improper encapsulation. • Authorization attacks, such as Password cracking or Token hacking could result in unauthorized access and system/data compromise. • Hotmail vulnerability– Microsoft was informed on August 29, 1999, of a weakness that allowed anyone to read the inbox of any Hotmail user, provided the username was known. • In February 1998, hackers launched an attack against the Pentagon and MIT. In the attack against MIT, hackers were able to collect

TECHNICAL THREATS (GSS)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
		user names and passwords to computers outside the network through the use of a packet sniffer. Details on the attack against the Pentagon were not made available.
10. Jamming (Telecommunications) ***System Impact*** *Primarily affects the availability of the system.*	Jamming is the deliberate radiation, reradiation, or reflection of electromagnetic energy, which could cause communications degradation, or total loss of the system.	• Jamming the radio frequency could produce electrical interference that prevents system operation.
11. Impersonation ***System Impact*** *Could impact confidentiality, integrity and availability.*	Impersonations are threats that often become enablers for other threats. Impersonation for physical access could include misuse of badges, key cards, personal Identification numbers (PIN), etc. Impersonation for electronic or system access could include use of others' identification and authentication information in an attempt to gain system privileges and access to system resources.	• Sharing of badges, key cards, and passwords could provide unauthorized access to sensitive information. • Masquerading, such as impersonation: false identity external to computer systems or playback and spoofing attacks could result in unauthorized access to sensitive data. • Social engineering, such as tricking employees into revealing passwords or other information could compromise a target system's security. • Forged email messages could reveal sensitive information.
12. Saturation of Communications or Resources ***System Impact*** *Could impact*	Saturation of communications or system resources is the condition in which a component of a system has	• Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks, such as network saturation attacks and bandwidth consumption attacks could result in system/data unavailability. • Sendmail buffer overflow weakness, pipe

TECHNICAL THREATS (GSS)		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
integrity and availability.	reached its maximum traffic handling capacity. Saturation of communications or system resources is a threat that creates an unstable environment, which could degrade communications capabilities and/or consume processor time (e.g., flooding the buffer).	attacks and MIMEbo could allow compromise at the root level
13. Tampering ***System Impact*** *Primarily affects the integrity and availability of the system.*	Tampering is an unauthorized modification that alters the proper functioning of equipment in a manner that degrades the security functionality the asset provides.	• Web hacks could deface a web site, or disable the web server functionality. • Domain Name Service hacks could prevent authorized users from properly accessing network or Internet resources.
14. Other Threats	(To be specified by system owner or developer)	

4. Index

The following index lists threats that might occur and the effect they could produce. This list should be utilized by those preparing Risk Assessments.

4.1 Index of Threats to MAs and Other Systems

4.1.1 Confidentiality

Threat Category	Section	Threat to Confidentiality
Human	2.1.2	Inadvertent Acts or Carelessness
	2.1.3	Impersonation
	2.1.4	Shoulder Surfing
	2.1.5	User Abuse or Fraud

	2.1.7	Espionage
Technical	2.2.1	Misrepresentation of Identity
	2.2.2	Intrusion or Unauthorized Access to System Resources
	2.2.3	Data/System Contamination
	2.2.4	Eavesdropping
	2.2.5	Insertion of Malicious Code, Software, or Database Modification
	2.2.6	Takeover of Authorized Session

4.1.2 Integrity

Threat Category	Section	Threat to Integrity
Human	2.1.1	Data Entry Errors or Omissions
	2.1.3	Inadvertent Acts or Carelessness
	2.1.5	User Abuse or Fraud
	2.1.6	Theft, Sabotage, Vandalism, or Physical Intrusions
Technical	2.2.2	Intrusion or Unauthorized Access to System Resources
	2.2.5	Insertion of Malicious Code, Software, or Database Modification
	2.2.7	System and Application Errors, Failures, and Intrusions not Properly Audited and Logged

4.1.3 Availability

Threat Category	Section	Threat to Availability
Human	2.1.2	Inadvertent Acts or Carelessness
	2.1.5	User Abuse or Fraud
	2.1.6	Theft, Sabotage, Vandalism, or Physical Intrusions
Technical	2.2.2	Intrusion or Unauthorized Access to System Resources
	2.2.5	Insertion of Malicious Code, Software, or Database Modification
	2.2.7	System and Application Errors, Failures, and Intrusions not Properly Audited and Logged

4.2 Index of Threats to GSSs

This section provides an index to those threats most likely to affect the confidentiality, integrity and availability of General Support Systems.

4.2.1 Confidentiality

Threat Category	Section	Threat to Confidentiality
Environmental	None	
Human	3.2.2	Improper Disposal of Sensitive Media
	3.2.3	Shoulder Surfing

	3.2.4	Inadvertent Acts or Carelessness
	3.2.5	Omissions
	3.2.7	Scavenging
	3.2.8	Theft, Sabotage, Vandalism, or Physical Intrusions
	3.2.9	User Abuse
	3.2.10	Espionage
Natural	None	
Technical	3.4.1	Data/System Contamination
	3.4.2	Compromising Emanations
	3.4.3	Corruption by System, System Errors, or Failures
	3.4.4	Eavesdropping
	3.4.5	Misuse of Known Software Weaknesses
	3.4.7	Insertion of Malicious Code, Software, or Database Modification
	3.4.8	Installation Errors
	3.4.9	Intrusion or Unauthorized Access to System Resources
	3.4.11	Misrepresentation of Identity/Impersonation

4.2.2 Integrity

Threat Category	Section	Threat to Integrity
Environmental	3.1.1	Environmental Conditions
	3.1.2	Electromagnetic Interference
Human	3.2.4	Inadvertent Acts or Carelessness
	3.2.5	Omissions
	3.2.8	Theft, Sabotage, Vandalism, or Physical Intrusions
	3.2.9	User Abuse
	3.2.12	Terrorism
Natural	None	
Technical	3.4.1	Data/System Contamination
	3.4.3	Corruption by System, System Errors, or Failures
	3.4.5	Misuse of Known Software Weaknesses
	3.4.6	Hardware / Equipment Failure
	3.4.7	Insertion of Malicious Code, Software, or Database Modification
	3.4.8	Installation Errors
	3.4.9	Intrusion or Unauthorized Access to System Resources
	3.4.11	Misrepresentation of Identity/Impersonation
	3.4.12	Saturation of Communications or Resources
	3.4.13	Tampering

4.2.3 Availability

Threat Category	Section	Threat to Availability

Environmental	3.1.1	Environmental Conditions
	3.1.2	Electromagnetic Interference
	3.1.3	Hazardous Material Accident
	3.1.4	Physical Cable Cuts
	3.1.5	Power Fluctuation
Human	3.2.1	Arson
	3.2.4	Inadvertent Acts or Carelessness
	3.2.5	Omissions
	3.2.6	Procedural Violation
	3.2.8	Theft, Sabotage, Vandalism, or Physical Intrusions
	3.2.9	User Abuse
	3.2.10	Espionage
	3.2.11	Labor Unrest
	3.2.12	Terrorism
	3.2.13	Riot/Civil Disorder
Natural	3.3.1	Natural Disaster
	3.3.2	Secondary Disaster
Technical	3.4.1	Data/System Contamination
	3.4.3	Corruption by System, System Errors, or Failures
	3.4.5	Misuse of Known Software Weaknesses
	3.4.6	Hardware / Equipment Failure
	3.4.7	Insertion of Malicious Code, Software, or Database Modification
	3.4.8	Installation Errors
	3.4.9	Intrusion or Unauthorized Access to System Resources
	3.4.10	Jamming (telecomm)
	3.4.11	Misrepresentation of Identity/Impersonation
	3.4.12	Saturation of Communications or Resources
	3.4.13	Tampering

5. Index

The following index lists threats and their relationship to the four categories (Environmental/Physical, Human, Natural, and Technical). This list should be utilized by those preparing Risk Assessments.

5.1 Correlation of Threats to the Four Categories for MAs and Other Systems

Threat Area	Environmental/ Physical Threat	Human Threat	Natural Threat	Technical Threat
Data Entry Errors or Omissions		X		
Inadvertent Acts or Carelessness		X		

Threat Area	Environmental/ Physical Threat	Human Threat	Natural Threat	Technical Threat
Impersonation		X		
Shoulder Surfing		X		
User Abuse or Fraud		X		
Theft, Sabotage, Vandalism, or Physical Intrusions		X		
Espionage		X		
Misrepresentation of Identity				X
Intrusion or Unauthorized Access to System Resources				X
Data/System Contamination				X
Eavesdropping				X
Insertion of Malicious Code, Software, or Database Modification				X
Takeover of Authorized Session				X
System and Application Errors, Failures, and Intrusions not Properly Audited and Logged				X

5.2 Correlation of Threats to the Four Categories for GSSs

Threat Area	Environmental/ Physical Threat	Human Threat	Natural Threat	Technical Threat
Environmental Conditions	X			
Electromagnetic Interference	X			
Hazardous Material Accident	X			
Physical Cable Cuts	X			
Power Fluctuation	X			
Secondary Disasters	X		X	
Arson		X		
Improper Disposal of Sensitive Media		X		
Shoulder Surfing		X		
Inadvertent Acts or Carelessness		X		
Omissions		X		
Procedural Violation		X		

Threat Area	Environmental/ Physical Threat	Human Threat	Natural Threat	Technical Threat
Scavenging		X		
Theft, Sabotage, Vandalism, or Physical Intrusions		X		
User Abuse		X		
Espionage		X		
Labor Unrest		X		
Terrorism		X		
Riot/Civil Disorder		X		
Natural Disaster			X	
Data/System Contamination				X
Compromising Emanations				X
Corruption by System, System Errors, or Failures				X
Eavesdropping				X
Misuse of Known Software Weaknesses				X
Hardware/Equipment Failure				X
Insertion of Malicious Code, Software, or Database Modification				X
Installation Errors				X
Intrusion or Unauthorized Access to System Resources				X
Jamming (telecomm*)*				X
Misrepresentation of Identity/Impersonation				X
Saturation of Communications or Resources				X
Tampering				X

6. Acronyms

Acronym	Description
CMS	Centers For Medicare & Medicaid Services
CPU	Central Processing Unit
CSS	Cross site Scripting
DOS	Denial Of Service
DDOS	Distributed Denial Of Service
EMI	Electromagnetic Interference
FTP	File Transfer Protocol
GSS	General Support System
IIS	Internet Information Server
IMAP	Internet Message Access Protocol
MA	Major Application
NFS	Network File System
OIS	Office of Information Services
PCs	Personal Computers
PIN	Personal Identification Number
POP	Post Office Protocol
RDS	Remote Data Services
RFI	Radio Frequency Interference
RPC	Remote Procedure Call
SSG	Security and Standards Group
SSN	Social Security Number
USERID	User Identification