JOINT BASE SAN ANTONIO (JBSA) CPCON CARD

CPCON 5-Normal Readiness. Characterized by routine NetOps, normal readiness of information systems and networks that can be sustained indefinitely. Information networks are fully operational in a known baseline condition. Item #: Task:

01 Verify your system is displaying "CPCON 5" upon log-on. If not, contact your unit ISSO.
02 Verify, **<u>at least every two weeks</u>**, if current anti-virus signatures are being automatically installed on your system. If you do not know how to verify the currency of the anti-virus, contact your unit ISSO.
03 **<u>Ensure to log out of the system and RESTART system at COB</u>**. This way your system can be scanned and patched for any known vulnerabilities.
04 Report any unusual system activity to your unit ISSO.
05 Review higher CPCON Levels.

CPCON 4- Increased Military Vigilance. Increased NetOps readiness, in preparation for operations or exercises, with a limited impact to the end-user
<u>Item #: Task:</u>

01 Continue to perform required tasks in lower CPCON levels.
02 Verify your system is displaying "CPCON 4" upon log-on. If not, contact your unit ISSO.
03 Update and revalidate the accuracy of user accounts and require a password change for all NIPRnet accounts not using 2-factor authentication.
04 Validate and update, manually or through automated means, the current definition of SIPRnet and NIPRnet anti-virus software.
05 Conduct user/operator training to increase situational awareness concerning "socially engineered" email and "phishing"activity.
06 Report all unusual system activity to your unit ISSO.
07 Review higher CPCON Levels.

CPCON 3-Enhanced Readiness. Further increase NetOps readiness by increasing the frequency of validation of the information network and its corresponding configuration. Impact to end-users is minor.
<u>Item #: Task:</u>

01 Continue to perform required tasks in lower CPCON levels.
02 Verify your system is displaying "CPCON 3" upon log-on. If not, contact your unit ISSO.
03 You may be asked to only use protected means of information exchange to discuss official business (such as secure phones, secure fax, or SIPRNet).
04 Limit the size of e-mail attachments to reduce network bandwidth use.
05 Review higher CPCON Levels.

CPCON 2–Greater Readiness. A readiness condition requiring a further increase in frequency of validation of the information network and its corresponding configuration. The impact on system administrators will increase in comparison to CPCON 3. Impact to end-users could be significant for short periods.
<u>Item #: Task:</u>

01 Continue to perform required tasks in lower CPCON levels. Verify
02 your system is displaying "CPCON 2" upon log-on. If not, contact your unit ISSO.
03 Identify to your ISSO any computer system that was disconnected from the network or compromised during the CPCON escalation.

CPCON 1–Maximum Readiness Highest readiness condition and addresses intrusion techniques that cannot be identified or defeated at lower readiness levels. Impact on systems administrators and users will be significant.
<u>Item #: Task:</u>

01 Continue to perform required tasks in lower CPCON levels.
02 Verify your system is displaying "CPCON 1" upon log-on. If not, contact your unit ISSO.
03 Identify to your ISSO any computer system that was disconnected from the network or compromised during the CPCON escalation.

JBSANANTONIOVA17-1301, 20230711 **OPR: 502 CS/SCXS**
(Per AFI 17-130) **Supersedes: JBSANANTONIOVA17-1301, 20190725**

There are no releasability restrictions on this publication

JOINT BASE SAN ANTONIO (JBSA) CPCON CARD

CPCON 5-Normal Readiness. Characterized by routine NetOps, normal readiness of information systems and networks that can be sustained indefinitely. Information networks are fully operational in a known baseline condition. Item #: Task:

01 Verify your system is displaying "CPCON 5" upon log-on. If not, contact your unit ISSO.
02 Verify, **<u>at least every two weeks</u>**, if current anti-virus signatures are being automatically installed on your system. If you do not know how to verify the currency of the anti-virus, contact your unit ISSO.
03 **<u>Ensure to log out of the system and RESTART system at COB</u>**. This way your system can be scanned and patched for any known vulnerabilities.
04 Report any unusual system activity to your unit ISSO.
05 Review higher CPCON Levels.

CPCON 4- Increased Military Vigilance. Increased NetOps readiness, in preparation for operations or exercises, with a limited impact to the end-user
<u>Item #: Task:</u>

01 Continue to perform required tasks in lower CPCON levels.
02 Verify your system is displaying "CPCON 4" upon log-on. If not, contact your unit ISSO.
03 Update and revalidate the accuracy of user accounts and require a password change for all NIPRnet accounts not using 2-factor authentication.
04 Validate and update, manually or through automated means, the current definition of SIPRnet and NIPRnet anti-virus software.
05 Conduct user/operator training to increase situational awareness concerning "socially engineered" email and "phishing"activity.
06 Report all unusual system activity to your unit ISSO.
07 Review higher CPCON Levels.

CPCON 3-Enhanced Readiness. Further increase NetOps readiness by increasing the frequency of validation of the information network and its corresponding configuration. Impact to end-users is minor.
<u>Item #: Task:</u>

01 Continue to perform required tasks in lower CPCON levels.
02 Verify your system is displaying "CPCON 3" upon log-on. If not, contact your unit ISSO.
03 You may be asked to only use protected means of information exchange to discuss official business (such as secure phones, secure fax, or SIPRNet).
04 Limit the size of e-mail attachments to reduce network bandwidth use.
05 Review higher CPCON Levels.

CPCON 2–Greater Readiness. A readiness condition requiring a further increase in frequency of validation of the information network and its corresponding configuration. The impact on system administrators will increase in comparison to CPCON 3. Impact to end-users could be significant for short periods.
<u>Item #: Task:</u>

01 Continue to perform required tasks in lower CPCON levels.
02 Verify your system is displaying "CPCON 2" upon log-on. If not, contact your unit ISSO.
03 Identify to your ISSO any computer system that was disconnected from the network or compromised during the CPCON escalation.

CPCON 1–Maximum Readiness Highest readiness condition and addresses intrusion techniques that cannot be identified or defeated at lower readiness levels. Impact on systems administrators and users will be significant.
<u>Item #: Task:</u>

01 Continue to perform required tasks in lower CPCON levels.
02 Verify y our system is displaying "CPCON 1" upon log-on. If not, contact your unit ISSO.
03 Identify to your ISSO any computer system that was disconnected from the network or compromised during the CPCON escalation.

JBSANANTONIOVA17-1301, 20230711 **OPR: 502 CS/SCXS**
(Per AFI 17-130) **Supersedes: JBSANANTONIOVA17-1301, 20190725**

There are no releasability restrictions on this publication

JOINT BASE SAN ANTONIO
(JBSA) CPCON CARD

NETWORK USER “Dos & DON’Ts

All network users help ensure network integrity by following the below “DOs & DON’Ts”. These are all common-sense items that, if adhered to, will guarantee network security & thwart all possible threat attempts by an unknown attacker.

01 **Be aware of your surroundings** & report suspicious behavior such as “shoulder surfing” or unauthorized access to sensitive or classified information. Challenge unknown personnel in your areas, especially when their behavior is questionable!

02 **Don’t ever leave your computer unattended** without using a password protected screen saver or logging off the network completely. Never leave your CAC unattended in your computer.

03 Protect your access to information from the insider threat: DO NOT share your password. DO NOT write your password down so it can be accessed easily. Remember the most common places people write their passwords down: (1) on the back of their keyboards, (2) bottom of their mouse, (3) posted on their wall, & (4) printed on a piece of paper laying in their desk drawer, are the first places an intruder will check.

04 A very large network threat is **Social Engineering**. Social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. Social engineering is a component of many, if not most, types of exploits. Virus writers use social engineering tactics to persuade people to run malware-laden email attachments, phishers use social engineering to convince people to divulge sensitive information, and scareware vendors use social engineering to frighten people into running software that is useless at best and dangerous at worst. If you are aware of any type of Social Engineering, immediately contact your Unit Information System Security Officer (ISSO), 502 CS CFP, and Client Support Administrator (CST).

05 **Phishing** is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. This is similar to *Fishing*, where the fisherman puts a bait at the hook, thus, pretending to be a genuine food for fish. Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. If you receive such an e-mail, immediately delete it & notify your CST or ISSO.

06 A common threat to our network is a **Distributed Denial of Service (DDoS)** attack. The most common of these attacks relate to e-mail. Beware of e-mail from unknown sources or known individuals with unusual subjects containing an attachment. Many DDoS attacks are triggered by an embedded script in the attachment that goes to your offline address book (OAB) & resends the same e-mail, with attachment, to everyone in your OAB. If you receive such an e-mail, immediately delete it & notify your CST or unit ISSO.

07 Other possible DDoS attacks relate to **Internet hoaxes**. These are warnings of new viruses, money making schemes, or chain letters. They all ask the users to forward the message to friends in the name of a fictitious cause. These types of attacks only slow down the Internet and e-mail service for computer users. Do not respond to these requests. Notify your CST or unit ISSO.

08 Make sure your **antivirus software is current**. Ensure your system is being scanned for viruses every week, at a minimum. Ensure you scan all removable media for viruses, before use. Common signs of viruses are: (1) Slow performance, (2) Files disappearing, (3) Constant computer error messages, (4) Erratic flashing, or (5) Constant e-mail error messages. If you experience any of these problems, contact your CST.

09 Negligent Discharge of Classified Information (NDCI), the inadvertent dissemination of classified information through the unclassified network (i.e. e-mail), are the most common form of a security incident. If you believe a (NDCI) has occurred, immediately notify your commander, Unit ISSO, Unit Security Manager/Unit Security Assistant and 502 CS CFP.

CONTACT INFORMATION

My ISSO is: ______________________________________ Ext: ___________

My CST is: ______________________________________ Ext: ___________

My FSA is: ____ Ext: _________

If you cannot contact the unit CST or ISSO, please contact the 502CS CFP at DSN 945-2666.

JOINT BASE SAN ANTONIO
(JBSA) CPCON CARD

NETWORK USER “Dos & DON’Ts

All network users help ensure network integrity by following the below “DOs & DON’Ts”. These are all common-sense items that, if adhered to, will guarantee network security & thwart all possible threat attempts by an unknown attacker.

01 **Be aware of your surroundings** & report suspicious behavior such as “shoulder surfing” or unauthorized access to sensitive or classified information. Challenge unknown personnel in your areas, especially when their behavior is questionable!

02 **Don’t ever leave your computer unattended** without using a password protected screen saver or logging off the network completely. Never leave your CAC unattended in your computer.

03 Protect your access to information from the insider threat: DO NOT share your password. DO NOT write your password down so it can be accessed easily. Remember the most common places people write their passwords down: (1) on the back of their keyboards, (2) bottom of their mouse, (3) posted on their wall, & (4) printed on a piece of paper laying in their desk drawer, are the first places an intruder will check.

04 A very large network threat is **Social Engineering**. Social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. Social engineering is a component of many, if not most, types of exploits. Virus writers use social engineering tactics to persuade people to run malware-laden email attachments, phishers use social engineering to convince people to divulge sensitive information, and scareware vendors use social engineering to frighten people into running software that is useless at best and dangerous at worst. If you are aware of any type of Social Engineering, immediately contact your Unit Information System Security Officer (ISSO), 502 CS CFP, and Client Support Administrator (CST).

05 **Phishing** is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. This is similar to *Fishing*, where the fisherman puts a bait at the hook, thus, pretending to be a genuine food for fish. Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. If you receive such an e-mail, immediately delete it & notify your CST or ISSO.

06 A common threat to our network is a **Distributed Denial of Service (DDoS)** attack. The most common of these attacks relate to e-mail. Beware of e-mail from unknown sources or known individuals with unusual subjects containing an attachment. Many DDoS attacks are triggered by an embedded script in the attachment that goes to your offline address book (OAB) & resends the same e-mail, with attachment, to everyone in your OAB. If you receive such an e-mail, immediately delete it & notify your CST or unit ISSO..

07 Other possible DDoS attacks relate to **Internet hoaxes**. These are warnings of new viruses, money making schemes, or chain letters. They all ask the users to forward the message to friends in the name of a fictitious cause. These types of attacks only slow down the Internet and e-mail service for computer users. Do not respond to these requests. Notify your CST or unit ISSO. .

08 Make sure your **antivirus software is current**. Ensure your system is being scanned for viruses every week, at a minimum. Ensure you scan all removable media for viruses, before use. Common signs of viruses are: (1) Slow performance, (2) Files disappearing, (3) Constant computer error messages, (4) Erratic flashing, or (5) Constant e-mail error messages. If you experience any of these problems, contact your CST.

09 Negligent Discharge of Classified Information (NDCI), the inadvertent dissemination of classified information through the unclassified network (i.e. e-mail), are the most common form of a security incident. If you believe a (NDCI) has occurred, immediately notify your commander, Unit ISSO, Unit Security Manager/Unit Security Assistant, and 502 CS CFP.

CONTACT INFORMATION

My ISSO is: ____Ext: _________

My CST is: ____Ext: _________

My FSA is: ____Ext: _________

If you cannot contact the unit CST or ISSO, please contact the 502CS CFP at DSN 945-2666.

JBSANANTONIOVA17-1301, 20230711 (Reverse)