My concerns with the question – 'have you ever intentionally mishandled classified information?'

1. Approximately 30-40% of my duties involve the transfer of classified data in support of national-level intelligence requirements, Special Operations planning and support to the war fighter. Because we use systems on both SIPRnet and JWICS, we are constantly moving data back and forth between them. This is accomplished via removable hard drive, DVD/CD and sometimes floppy disk. Usually, imagery and other data is acquired on the JWICS and moved down to the SIPRnet or standalone workstation for processing, and then moved back up to the JWICS for dissemination. Occasionally, some files are required to be downloaded from the JWICS only to disseminate on the SIPRnet. Another aspect is that some of our workstations are stand-alone and not connected to a network. As far as I know, they've never been officially designated as classified, but we use classified information on them, so we've internally designated them as classified – at one time several years ago as Top Secret, then more recently as Secret. Confusion usually arises as to what we should classify the removable media taken from these machines, ultimately developing in to feelings of inappropriate behavior. At one point we've heard that it's okay to mark a CD Secret if it only contains Secret data, but was taken from the JWICS. Then later we find out that it should have been marked Top Secret. We've also been instructed to document each and every file that is moved down from JWICS on a spreadsheet for accountability purposes. This spreadsheet currently consists of thousands and thousands of files. Although I have diligently tried to keep up with this list, due to overwhelming circumstances, I cannot state with a clear conscience that every single file that has been moved down has made it to the list. As a side note, we have never been required to provide this list to anyone.

2. Over the course of the last 12 years, we have been authorized to move data in this way, and then told to stop (BUCKSHOT YANKEE), and then told it was okay. Often times there were grey areas where we weren't exactly sure what we were doing was officially authorized, but in the interest of supporting the war fighter, we went ahead and moved the data. In the early 2000's, we were even told that we had an 'exception to policy' that authorized us to move classified data via removable media. Although I had never seen this 'exception to policy', I often felt that have been in some way circumventing the approved methods. Later, I was directed to self study for the Information Transfer Authority (ITA) test. The way this test worked was that you had to score at least 90% and you could only take it three times – the third failure would result in denial of the

authority. After falling short on the first two attempts, I decided that I would put off taking the test for the third time for as long as possible. This decision allowed us to continue transferring data without interruption for at least another few weeks. After being contacted by the Information Assurance Office on several occasions that they would have to lock down our machines if we weren't ITA certified, I studied intensely, took the test for the third time and finally passed.

3. Throughout the history of this office, we have been required to burn CDs/DVDs/floppy disks from either JWICS or SIPRnet and label them according to their contents. Up until about a year ago, this was accepted practice – depending on who you listened to. Some people would say it was fine, while others said that the removable media should be labeled with the level of classification of the system it came from. I was always uncomfortable with this practice and would always do it in trepidation. Now, according to SOCOM regulations, we have permission to create a disk with the classification of the system it was taken from, but not allowed to create and label a disk with a lower classification than the system it was taken from. Instead, a form 14 and an ECR is required before J6 representatives will perform the procedure for the requestor.

4. To help remedy these types of problems and address potential areas of concern to conscionable workers like me, SOCOM JICSOC leaders have directed J6 computer support personnel to create a workstation that has all the necessary applications on the JWICS. Although this would seem like an easy task, we have been waiting for over two years for the workstations to come online. In the meantime, we continue to transfer classified data back and forth between the domains adhering to current security requirements. Even when/if this gets accomplished, we will still face the dilemma of transferring down to SIPRnet for dissemination to the war fighter.

John S. Morter, GS-13
HQ USSOCOM, J2-JIC-GEOINT