COMPUTING SERVICES
Section: 135-3 APPENDIX C
Effective: 01/17/2012
Supersedes: 04/15/2010
Review Date: TBD
Issuance Date: 01/17/2012
Issuing Office: Administrative Computing & Telecommunications (ACT)

APPENDIX C – RISKY FILE TYPES

File Extension	Description
.ani	Windows animated cursor file security vulnerability. Possible buffer overflow in Windows
.bat	Batch files are often malicious
.bmp	Windows bitmap file security vulnerability. Possible buffer overflow in Windows
.cab	Possible malicious Microsoft cabinet file
.cer	Dangerous Security Certificate (according to Microsoft Q883260)
.chm	Complied help files are very dangerous in email
.cmd	Batch files are often malicious
.cnf	Speed Dials are very dangerous in email
.com	Executable DOS/Windows Programs are dangerous in email
.cpl	Control panel items are often used to hide viruses
.cur	Windows cursor file security vulnerability. Possible buffer overflow in Windows
.exe	Executable DOS/Windows programs are dangerous in email
.hlp	Windows file security vulnerability. Possible buffer overflow in Windows
.hta	HTML archives are very dangerous in email
.ico	Windows icon file security vulnerability. Possible buffer overflow in Windows
.ins	Windows Internet Settings are dangerous in email
.its	Dangerous Internet Document Set (according to Microsoft Q883260)
.job	Task Scheduler requests are dangerous in email
.jse*	JScript Scripts are dangerous in email
.lnk	Eudora .lnk security hole attack
.mad	Microsoft Access Shortcuts are dangerous in email
.maf	Microsoft Access Shortcuts are dangerous in email
.mag	Microsoft Access Shortcuts are dangerous in email
.mam	Microsoft Access Shortcuts are dangerous in email
.maq	Microsoft Access Shortcuts are dangerous in email

.mar	Microsoft Access Shortcuts are dangerous in email
.mas	Microsoft Access Shortcuts are dangerous in email
.mat	Microsoft Access Shortcuts are dangerous in email
.mau	Dangerous attachment type (according to Microsoft Q883260)
.mav	Microsoft Access Shortcuts are dangerous in email
.maw	Microsoft Access Shortcuts are dangerous in email
.mda	Dangerous attachment type (according to Microsoft Q883260)
.mdz	Dangerous attachment type (according to Microsoft Q883260)
.mhtl	MHTML files can be used in an attack against Eudora
.pif	Shortcuts to MS-Dos programs are very dangerous in email
.prf	Dangerous Outlook Profile Settings (according to Microsoft Q883260)
.pst	Dangerous Office Data File (according to Microsoft Q883260)
.reg	Windows registry entries are very dangerous in email
.scf	Windows Explorer Commands are dangerous in email
.scr	Windows Screensavers are often used to hide viruses
.sct	Windows Script Components are dangerous in email
.shb	Shortcuts Into Documents are very dangerous in email
.shs	Shell Scrap Objects are very dangerous in email
.tmp	Dangerous Temporary File (according to Microsoft Q883260)
.vbe	Visual Basic Scripts are dangerous in email
.vbs	Visual Basic Scripts are dangerous in email
.vsmacros	Dangerous Visual Studio Macros (according to Microsoft Q883260)
.vss	Dangerous attachment type (according to Microsoft Q883260)
.vst	Dangerous attachment type (according to Microsoft Q883260)
.vsw	Dangerous attachment type (according to Microsoft Q883260)
.wmf	Windows Metafile security vulnerability
.ws	Dangerous Windows Script (according to Microsoft Q883260)
.wsc	Windows Script Host files are dangerous in email
.wsf	Windows Script Host files are dangerous in email
.wsh	Windows Script Host files are dangerous in email
.xnk	Microsoft Exchange Shortcuts are dangerous in email
.zip	Compressed and packaged files used to distribute many virus/trojans
.txt.exe	Attachments using multiple extensions
filename.{1CE8B2C9-EAEF-43fc-8218-F092E4F94A47}	Format of Windows Class Identifiers (CLSID) The CLSID will not usually be displayed to the user. Windows may run the program that is associated with the CLSID if the user attempts to open the file.