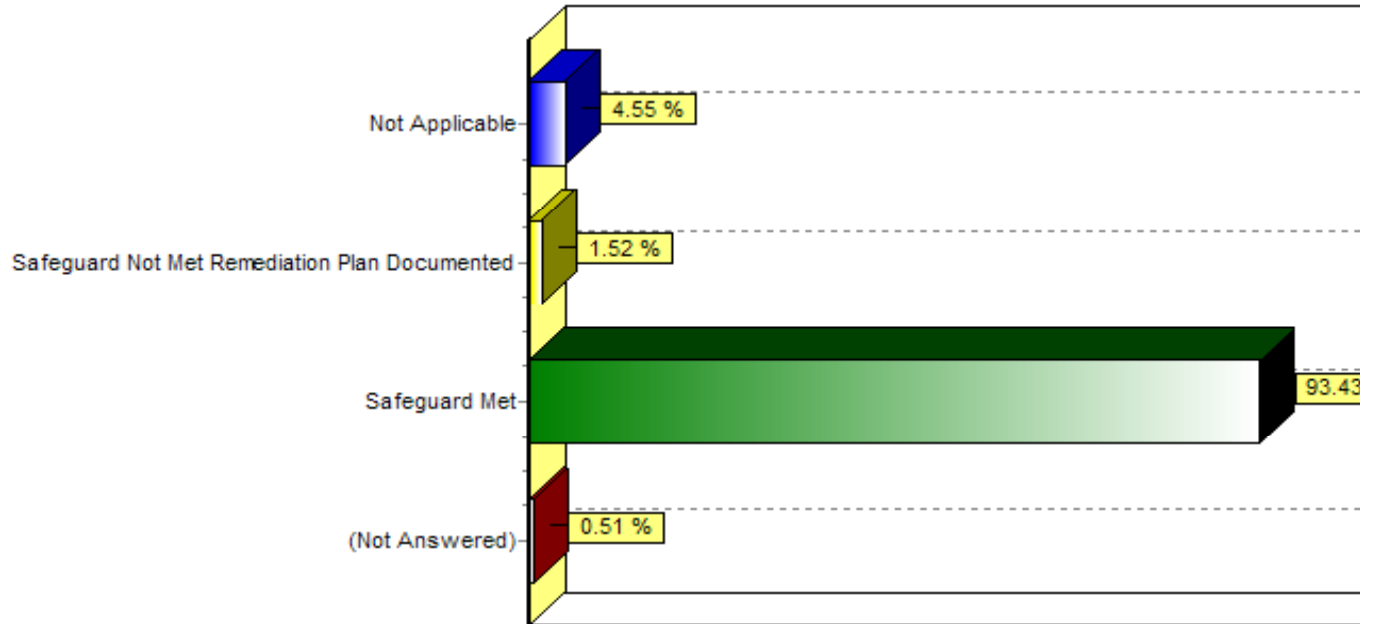


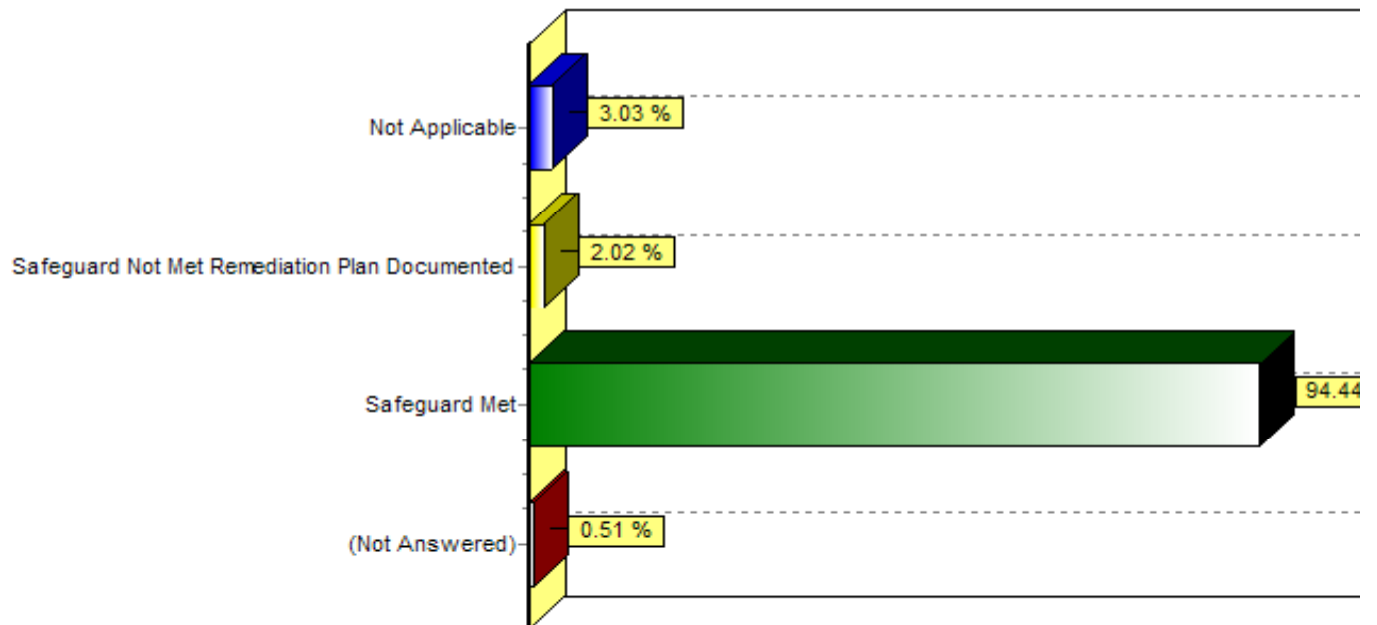
Bar Graphs

DHS Safeguards Assessment Tool 2005

A1. Access to areas with confidential materials are monitored or locked to prevent unauthorized entrance



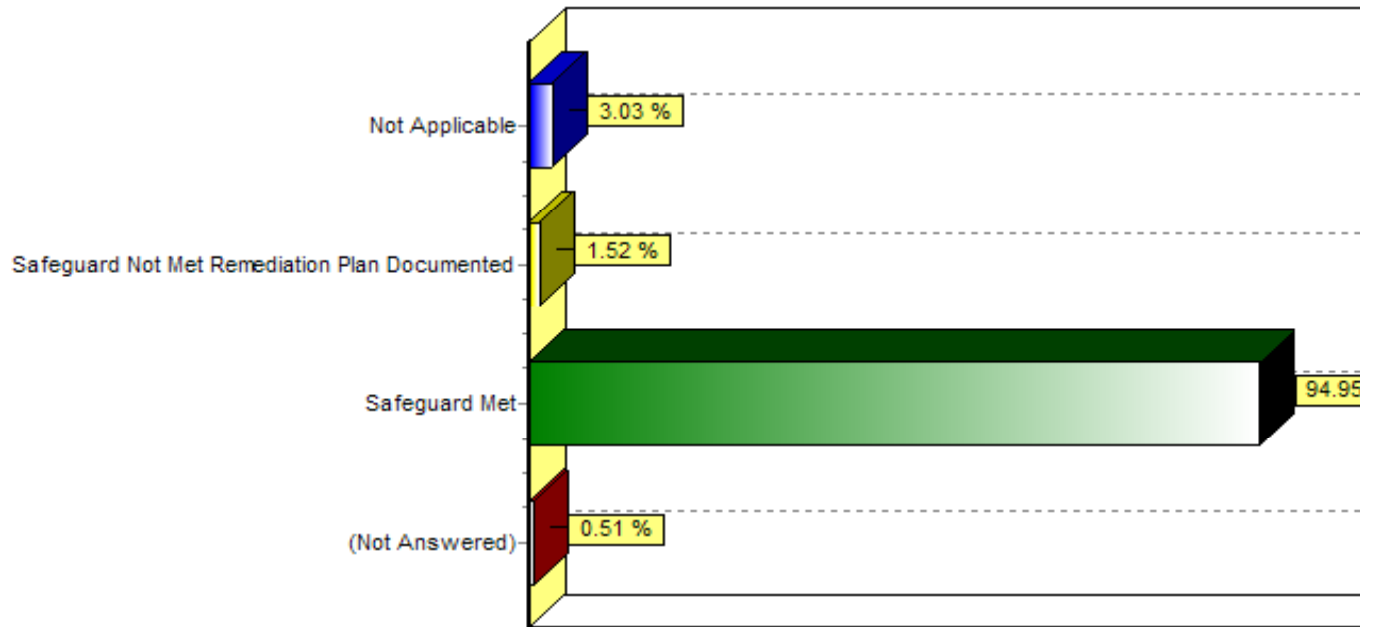
A2. Keys, keypad combinations, and key cards are controlled to assure only staff authorized by management have building access and/or after hours access.



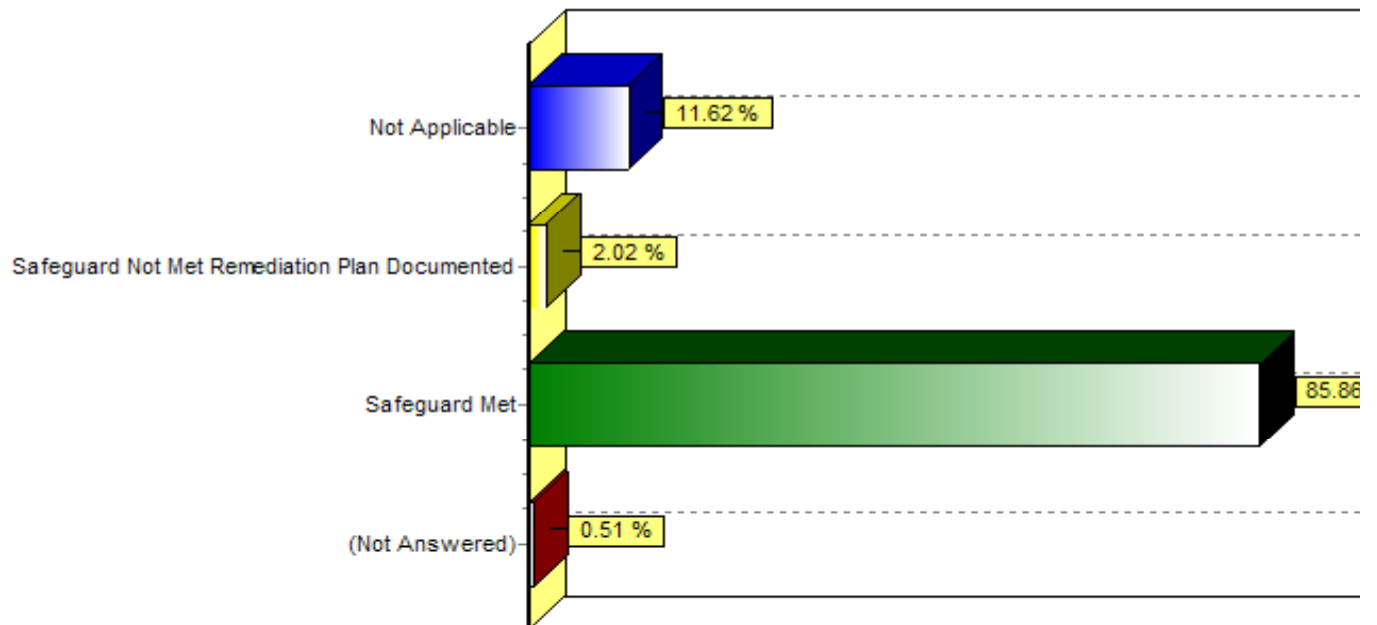
Bar Graphs

DHS Safeguards Assessment Tool 2005

A3. Work place discussions of confidential information are conducted in private locations or in voice levels that inhibit casual eavesdropping.



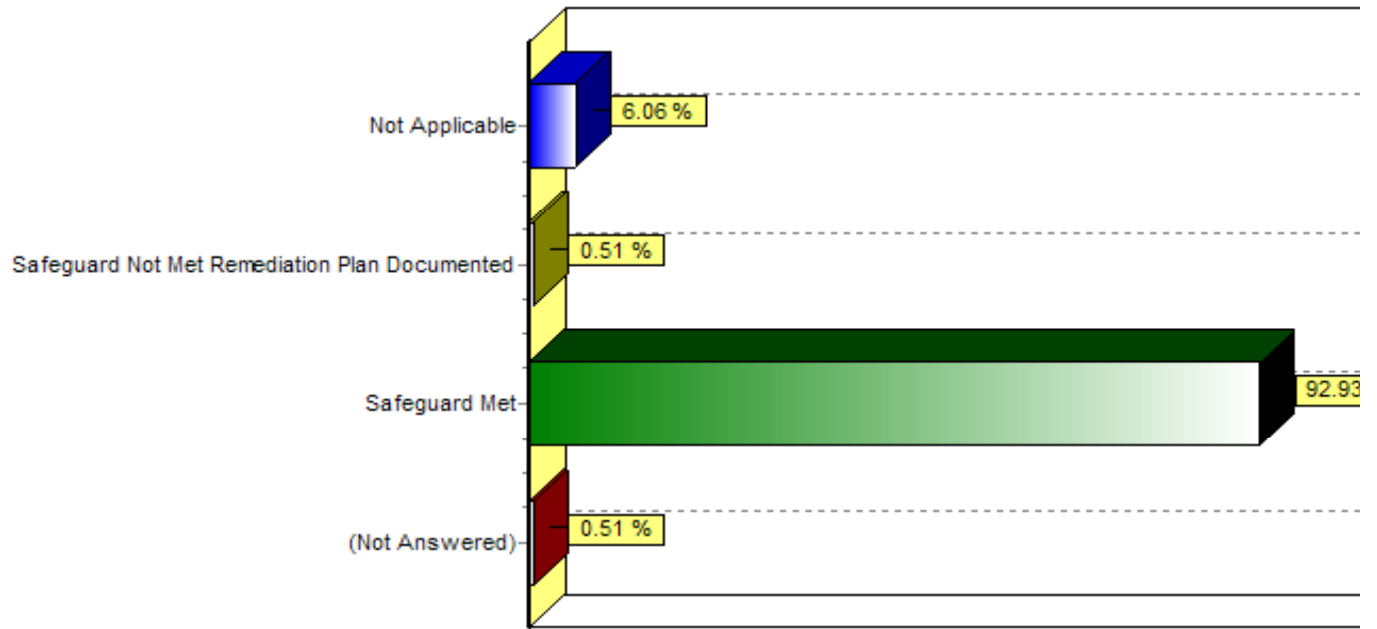
A4. A physical barrier separates reception and work areas, where necessary and appropriate.



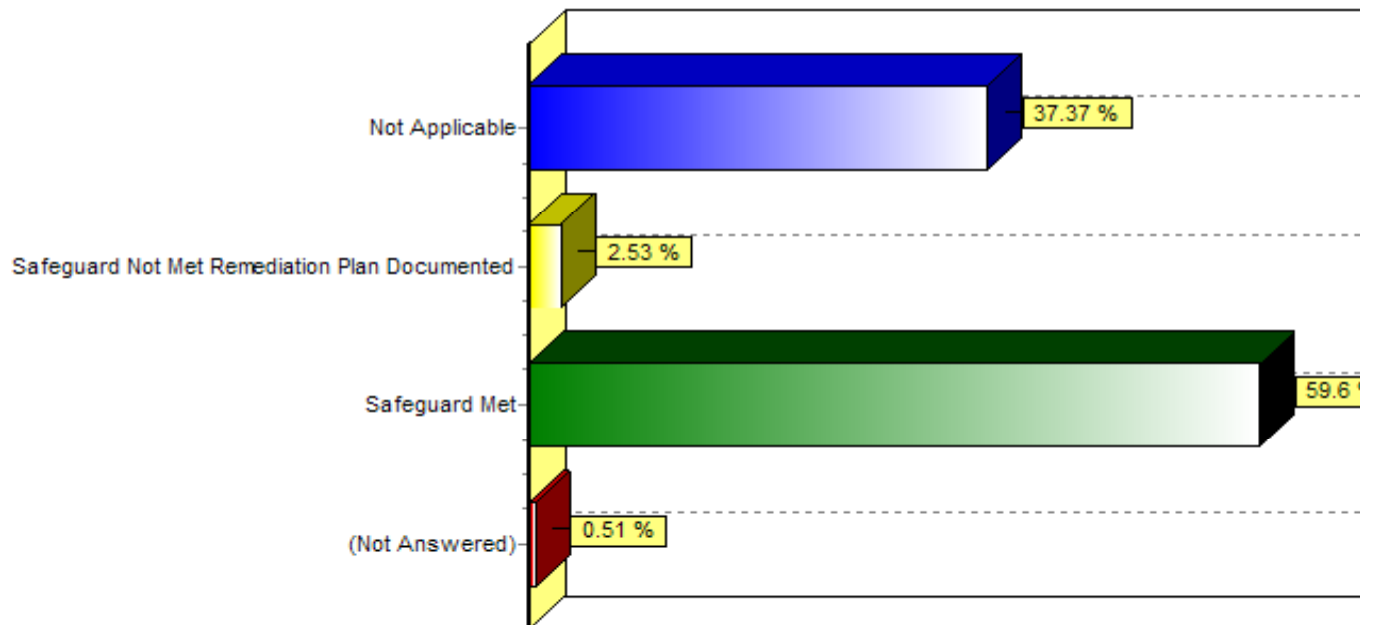
Bar Graphs

DHS Safeguards Assessment Tool 2005

B1. Building or work area process/policy for escorting non-DHS visitors in areas with confidential information is followed.



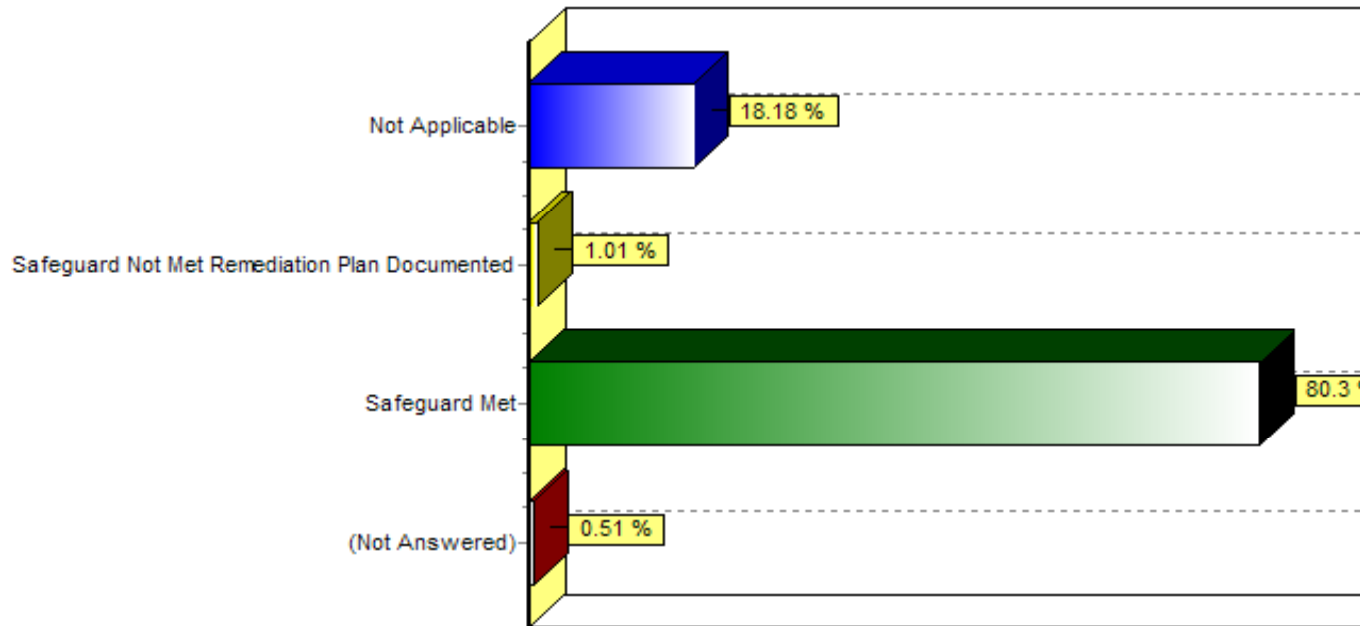
B2. If there is a building policy requiring ID to enter work area, it is enforced.



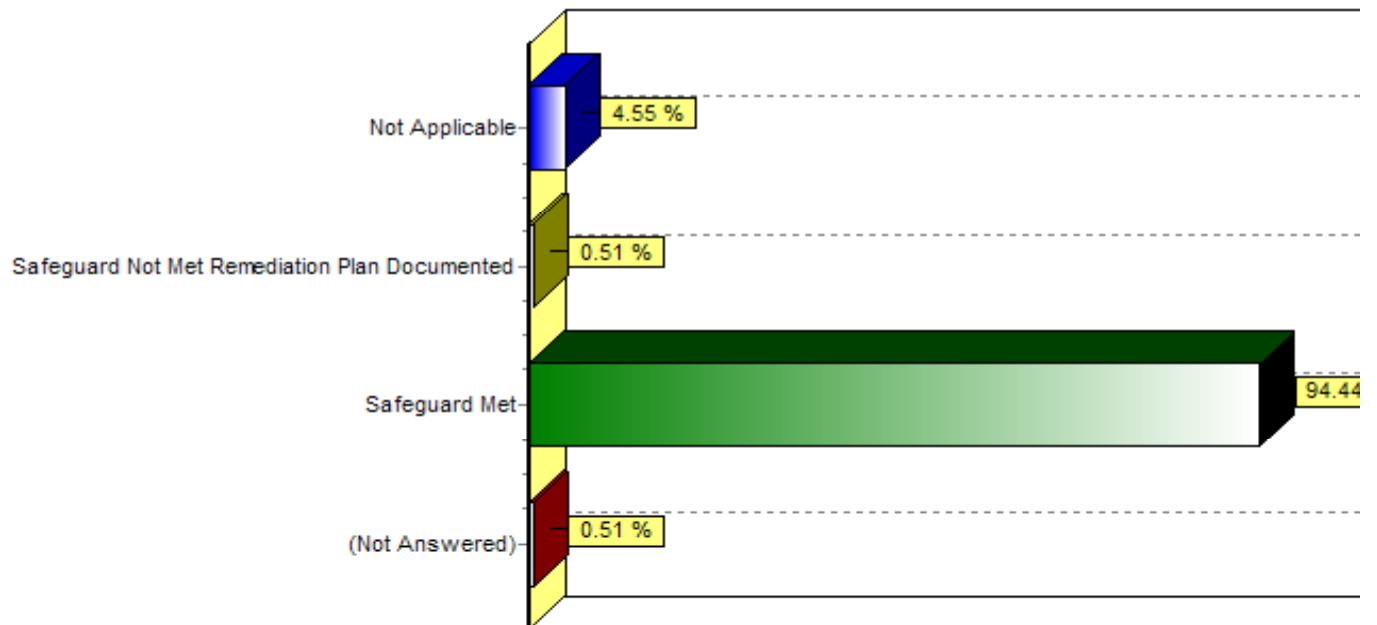
Bar Graphs

DHS Safeguards Assessment Tool 2005

B3. Contractors have completed confidentiality agreements.



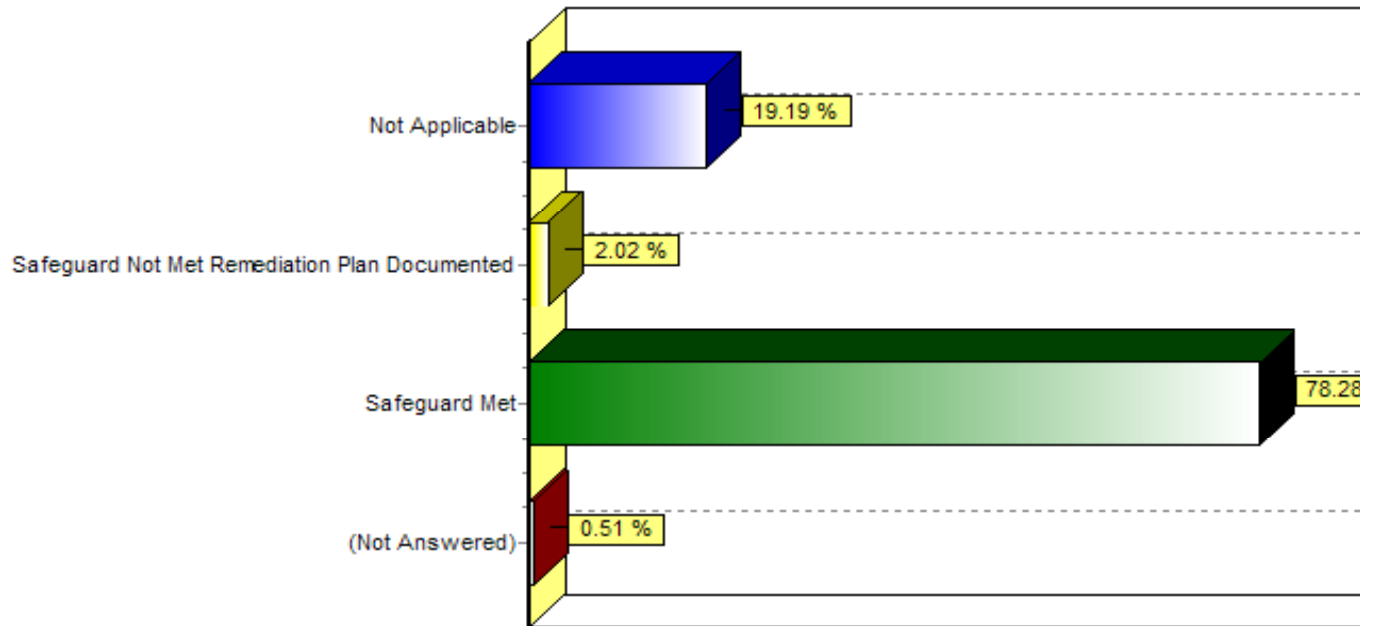
B4. Employees use reasonable measures, such as speaking in a soft voice, when discussing confidential issues in public areas.



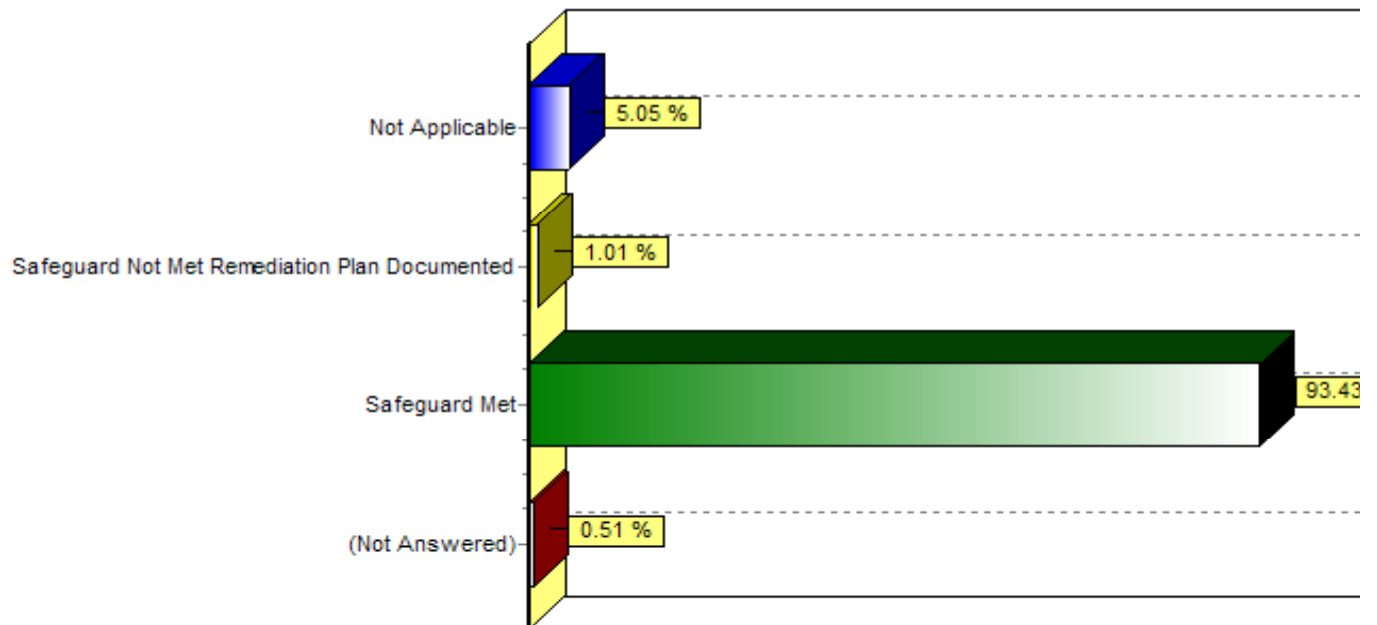
Bar Graphs

DHS Safeguards Assessment Tool 2005

B5. Janitorial staff are allowed access after hours only after completing a confidentiality agreement.



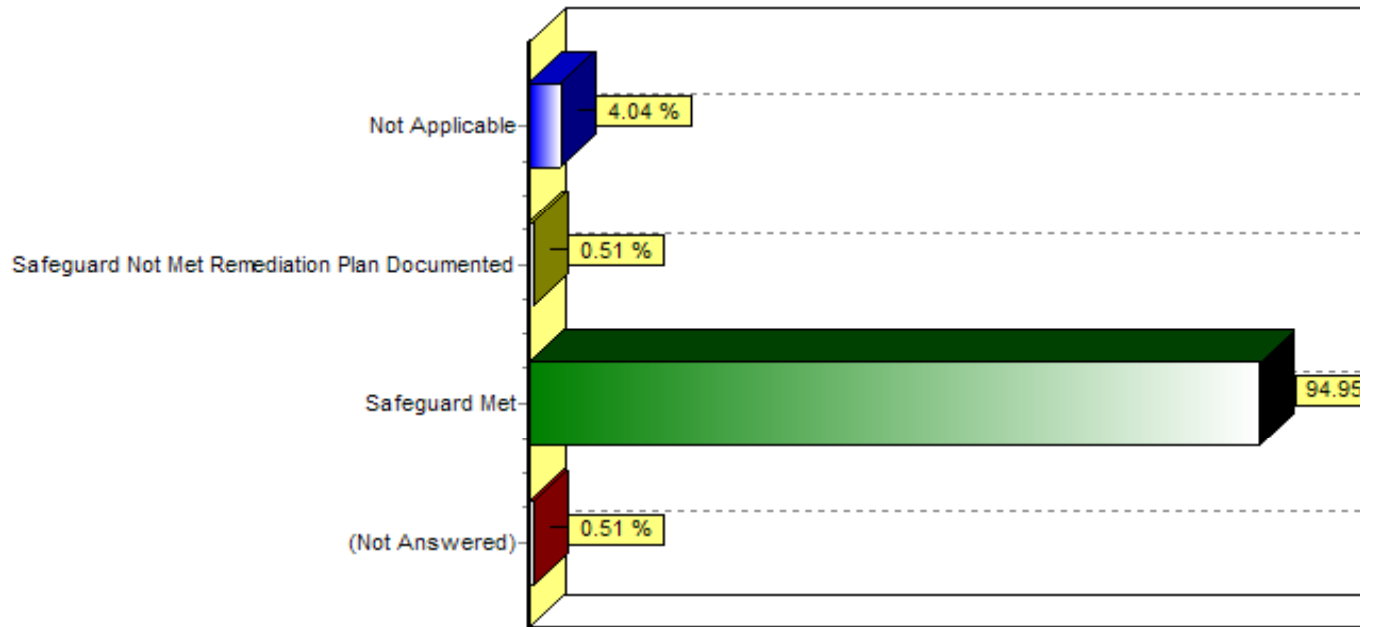
C1. The office has reasonable physical safeguards, such as partitions, view-limiting screen filters, or repositioning monitors to prevent unauthorized viewing of screens.



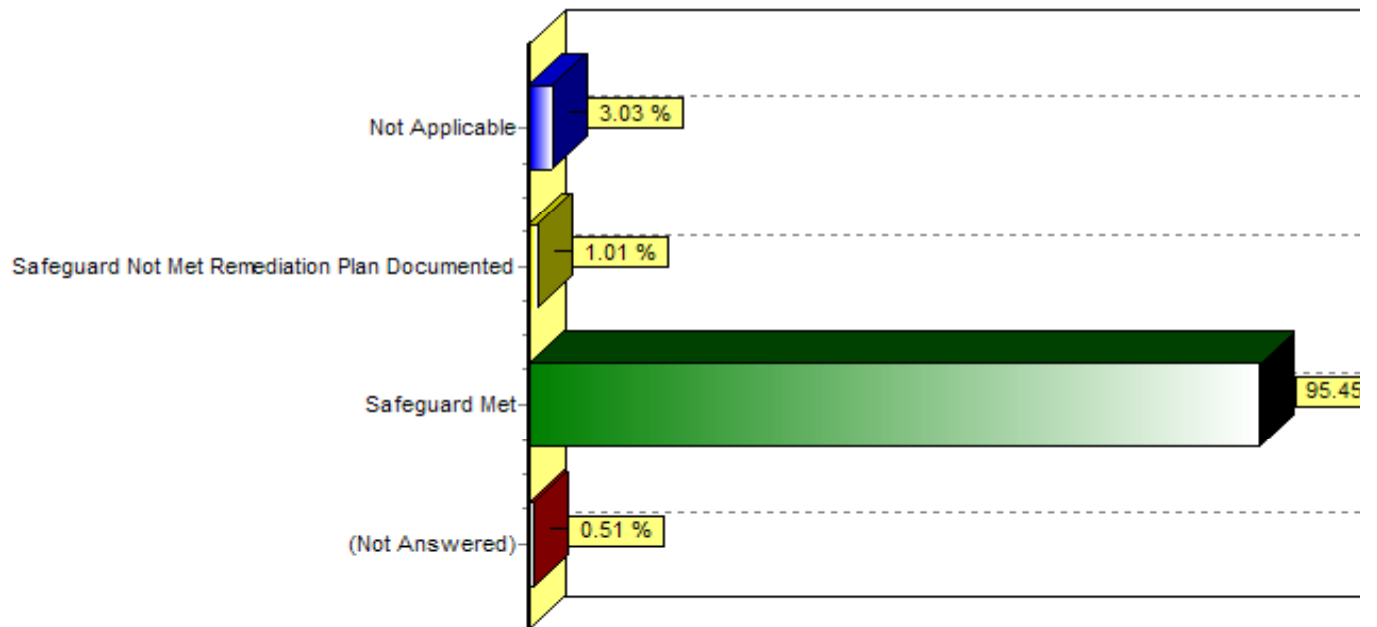
Bar Graphs

DHS Safeguards Assessment Tool 2005

C2. Staff exit applications or systems that have confidential information or lock their workstation upon leaving their cubicle or workspace.



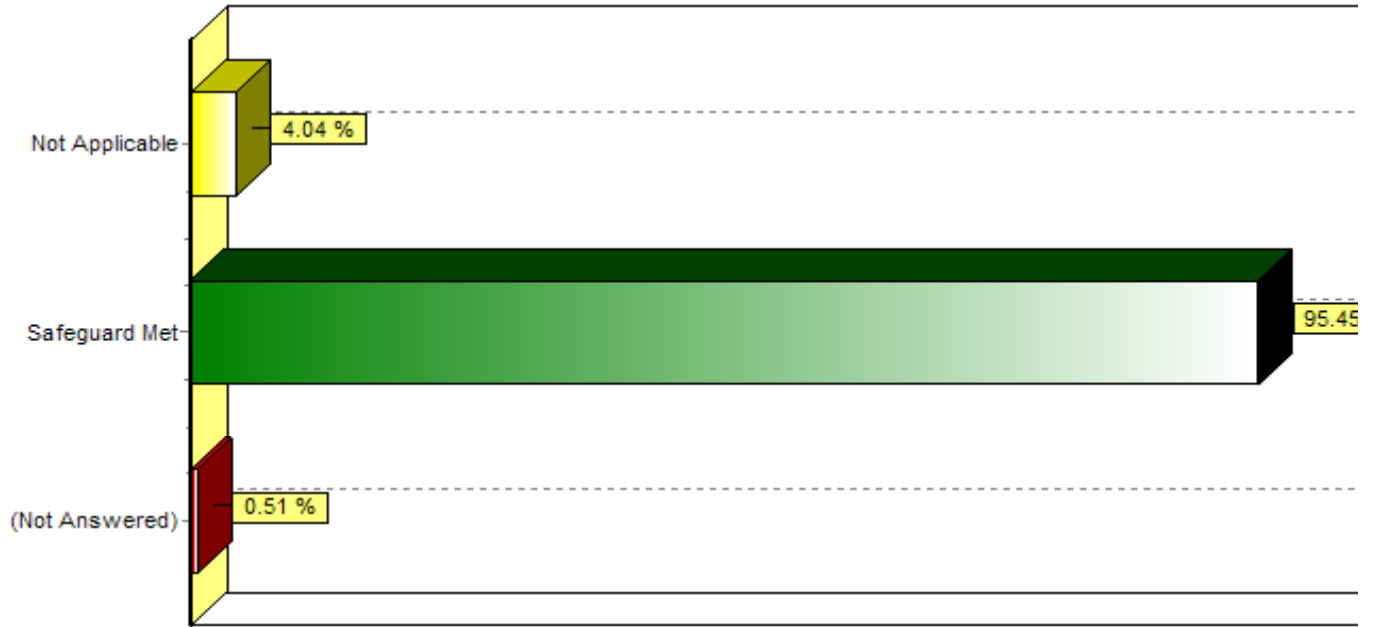
C3. Office equipment such as fax machines, printers, and copiers are located away from unsupervised public areas to prevent inadvertent access.



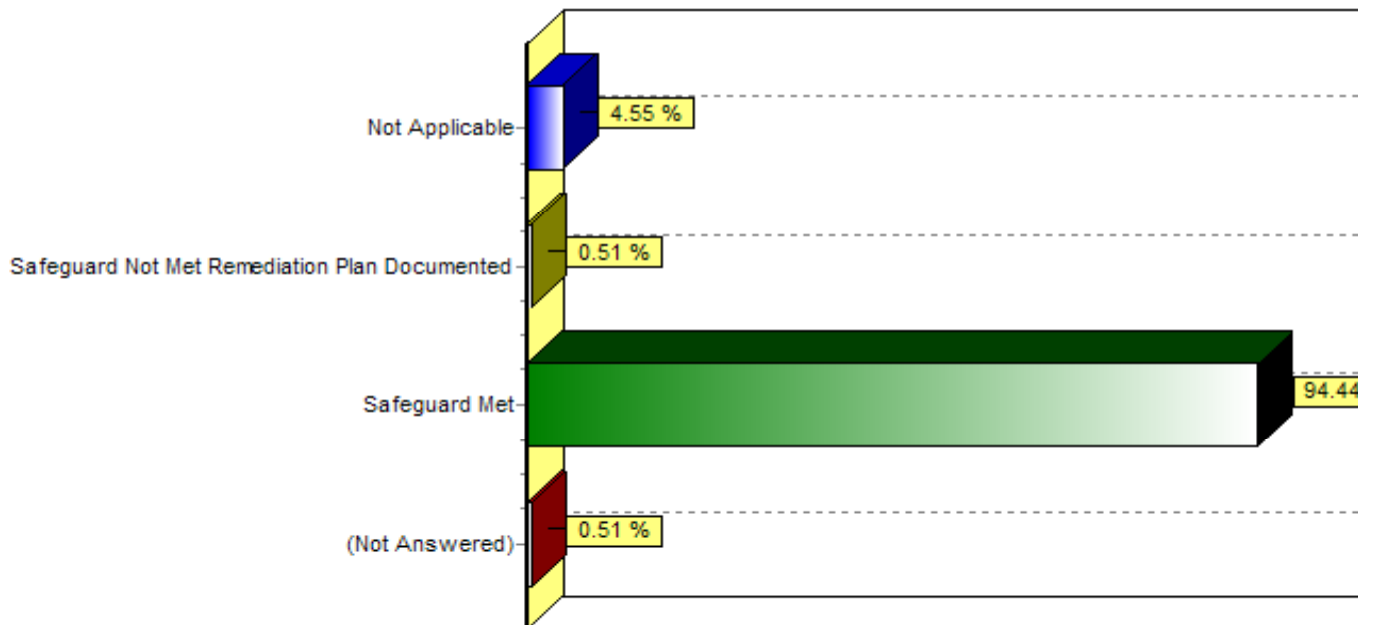
Bar Graphs

DHS Safeguards Assessment Tool 2005

C4. Office distributes confidential incoming faxes and materials left at copiers and printers timely, but at least within the workday.



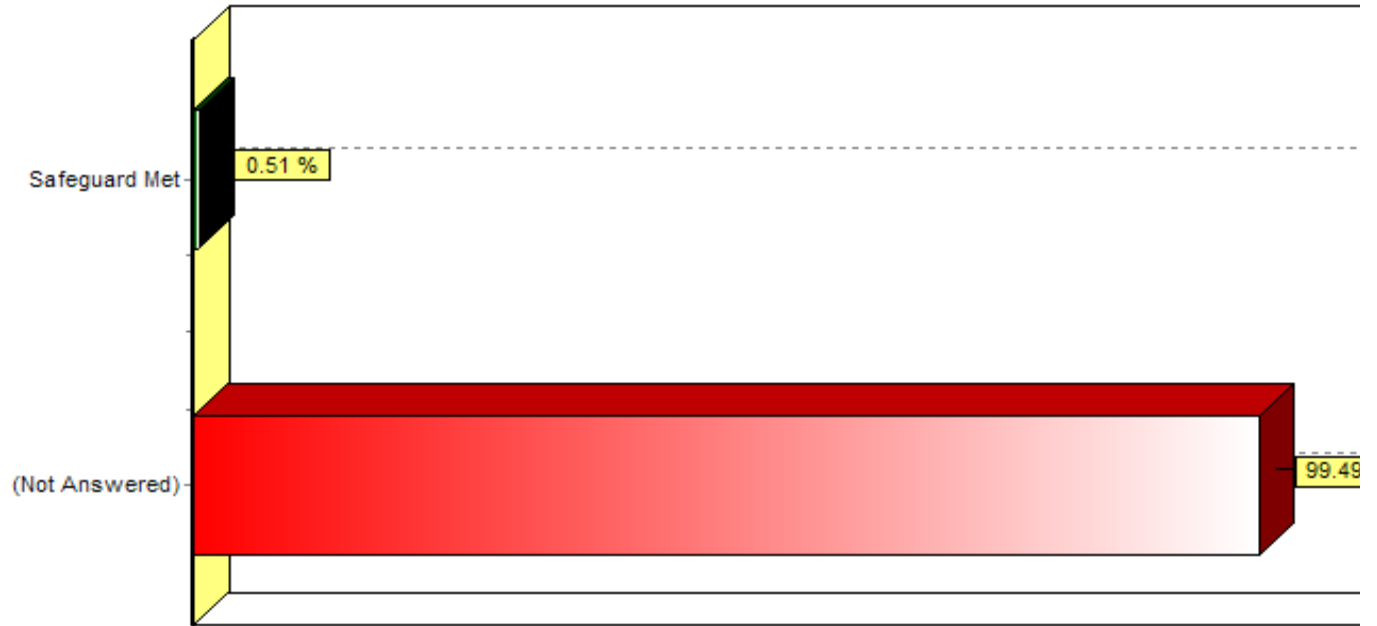
C5. Outgoing faxes include a cover page with the DHS privacy disclaimer.



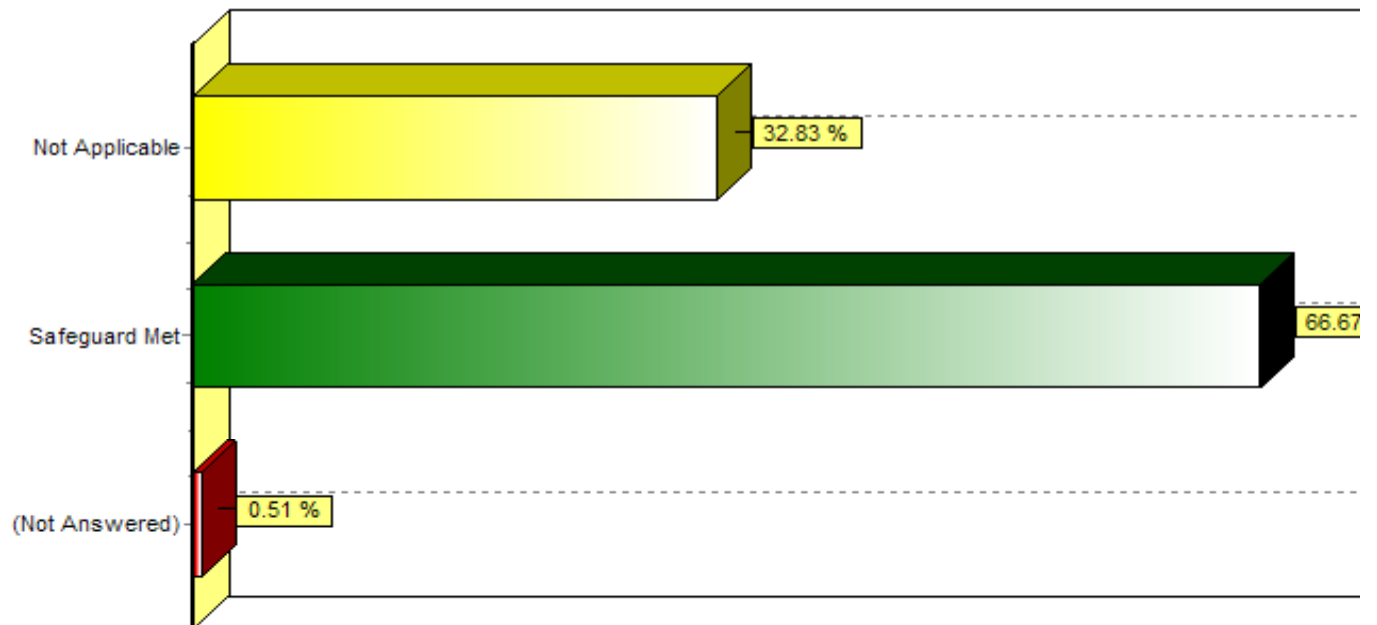
Bar Graphs

DHS Safeguards Assessment Tool 2005

C6. Outgoing faxes include a cover page with the DHS privacy disclaimer.



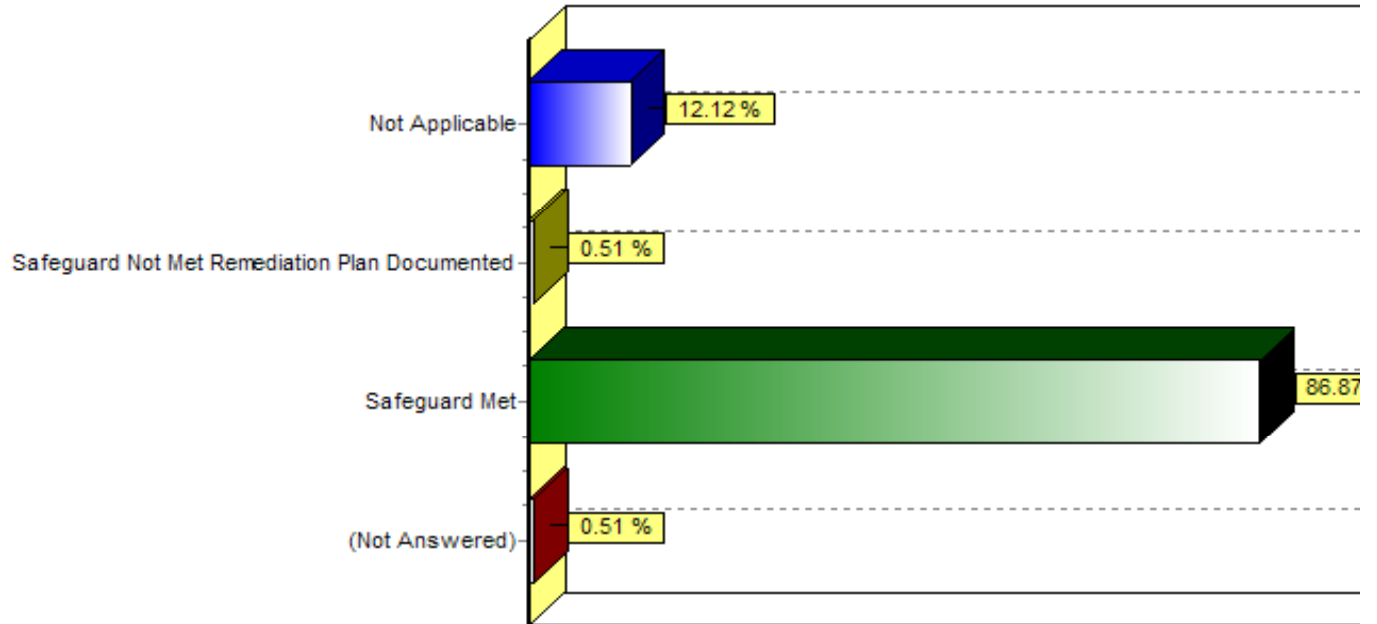
D1. When not in use, tapes, disks, CD-ROM's, Zip Drives and cartridges containing confidential material are secured in a locked cabinet, room or other secured location.



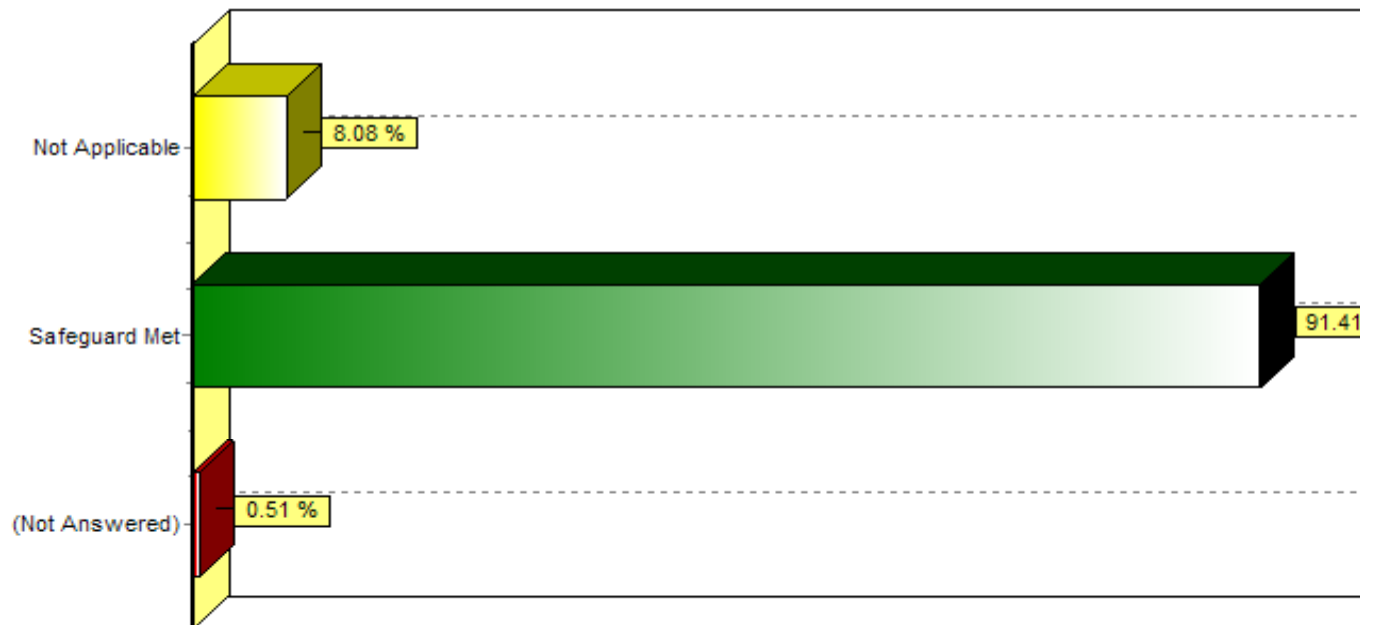
Bar Graphs

DHS Safeguards Assessment Tool 2005

D2. Only authorized staff has access to secure data locations, per DHS policy.



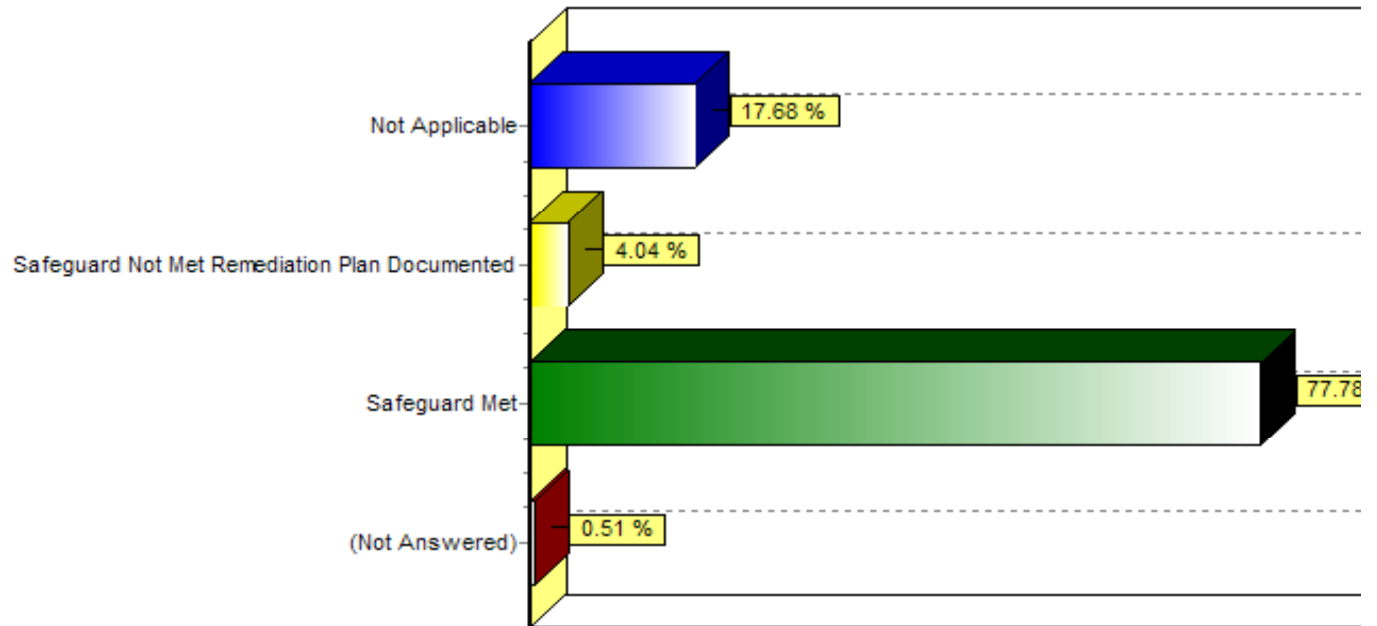
D3. Staff complies with office procedures that prohibit confidential data removal from office except as authorized.



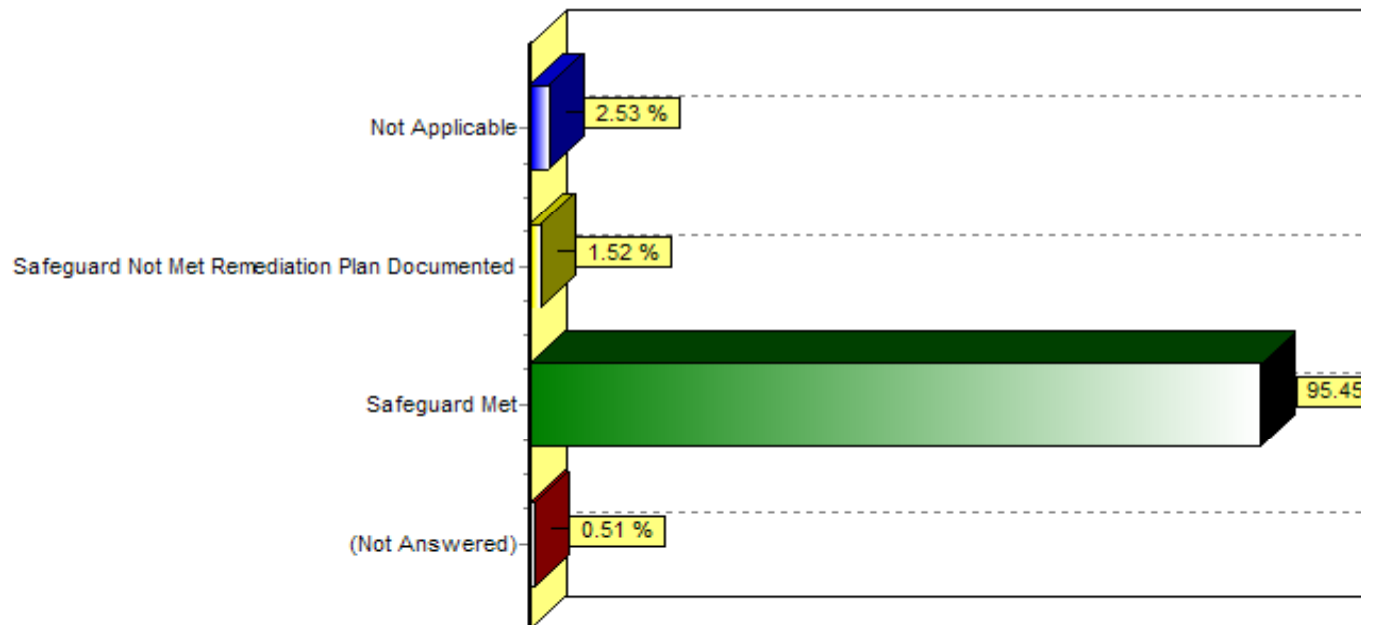
Bar Graphs

DHS Safeguards Assessment Tool 2005

D4. Information users are required to sign compliance statement as condition of access approval.



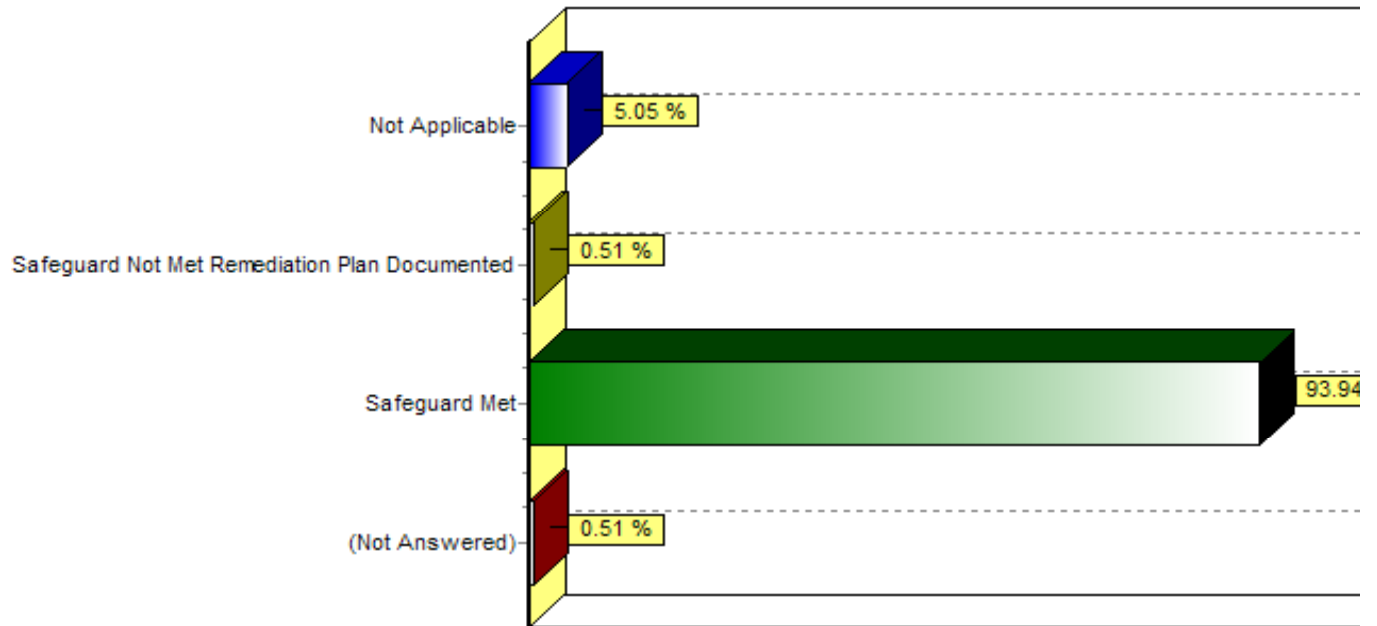
E1. Confidential materials are stored in locked rooms, secured storage systems or where lockable storage is not available, reasonable efforts are taken to safeguard files in accordance with the DHS policy.



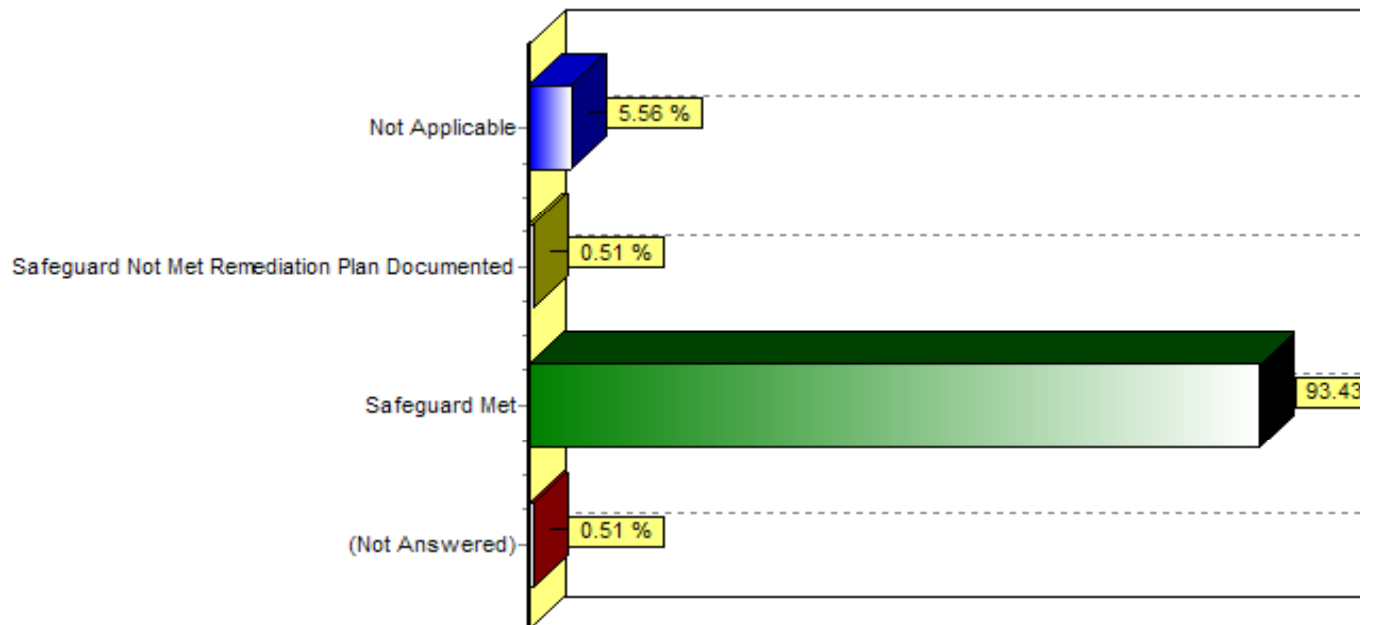
Bar Graphs

DHS Safeguards Assessment Tool 2005

E2. Only employees with authorization can access secured file rooms, cabinets or desks.



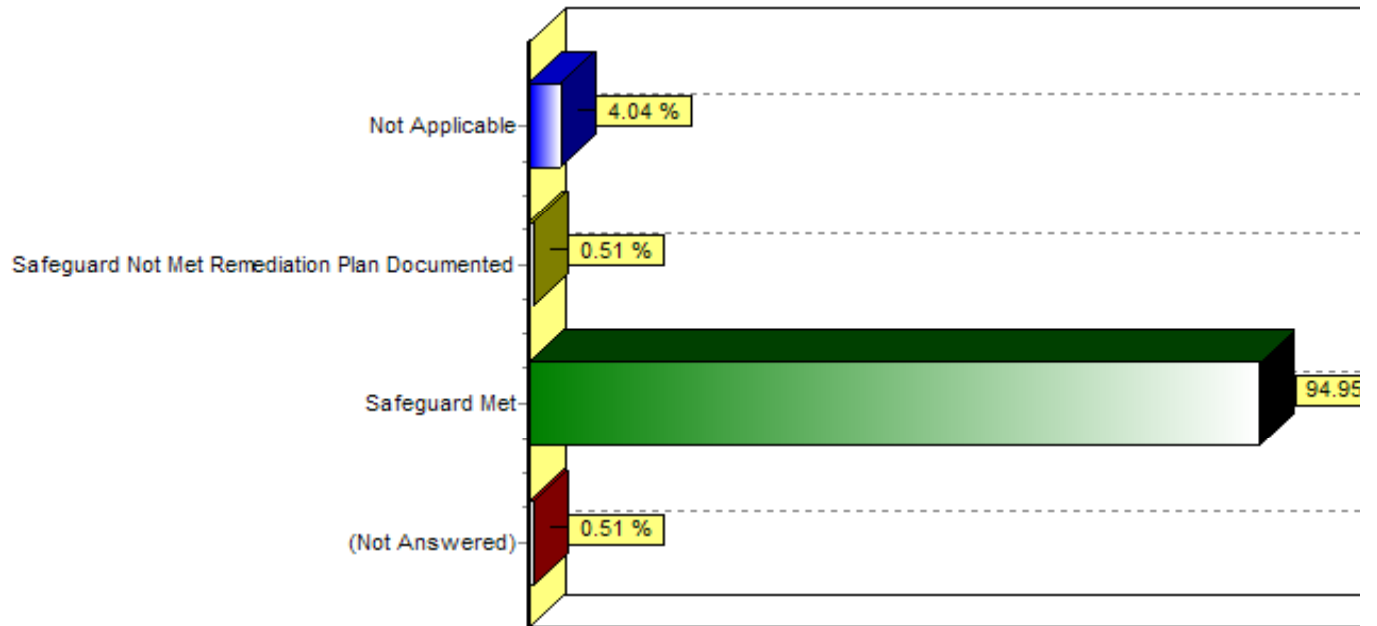
E3. File cabinets containing confidential materials are secured when not in use.



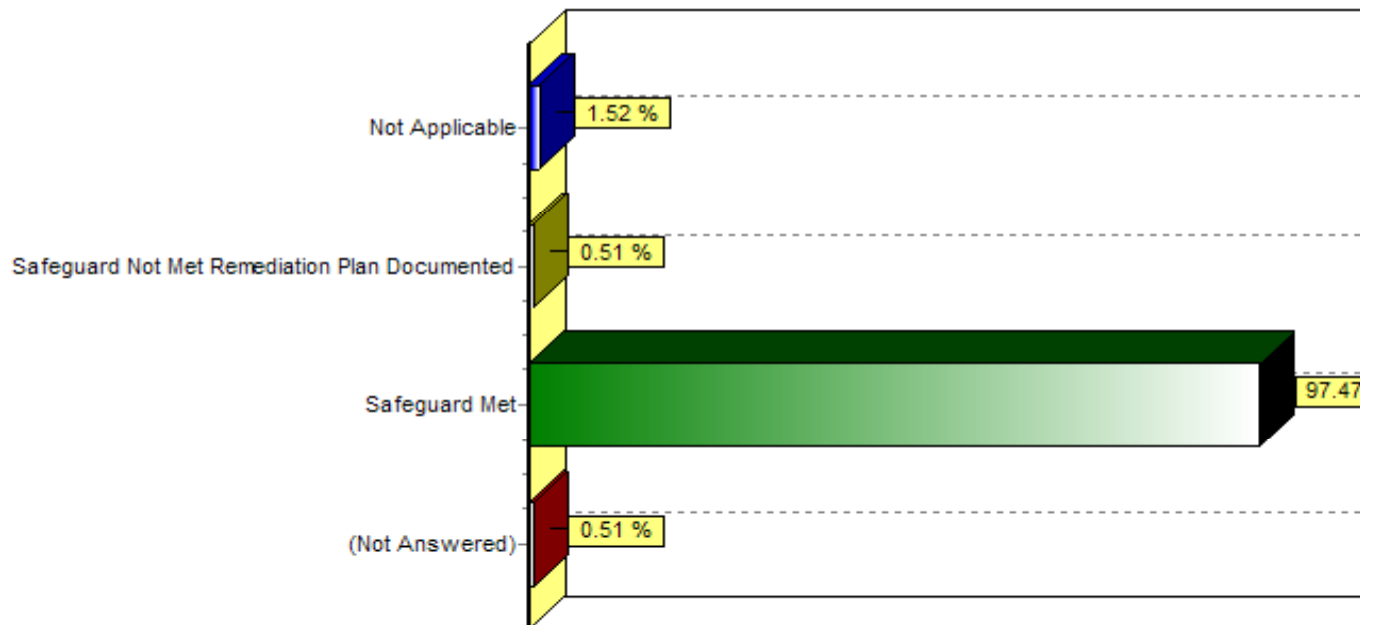
Bar Graphs

DHS Safeguards Assessment Tool 2005

E4. Access to file cabinets or files is secured from access by unauthorized persons.



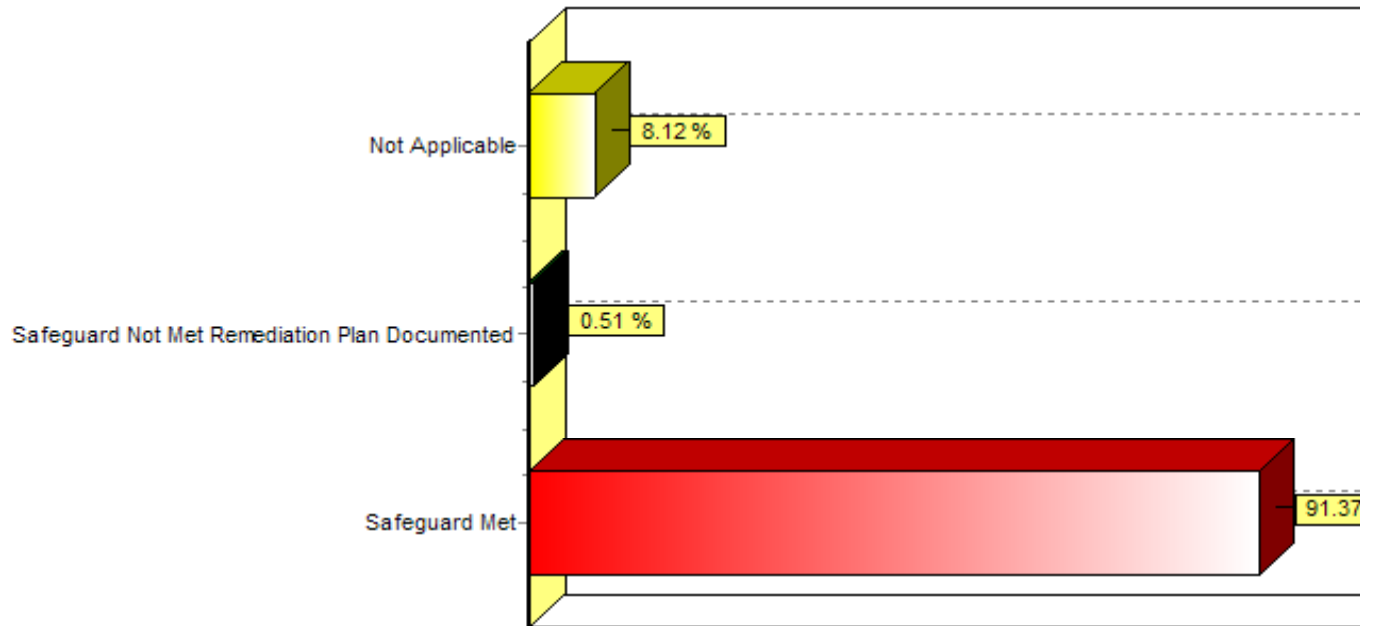
E5. In keeping with DHS policy, confidential materials on desktops, tables, printers, copiers, fax machines will be adequately shielded from visual inspection by unauthorized parties.



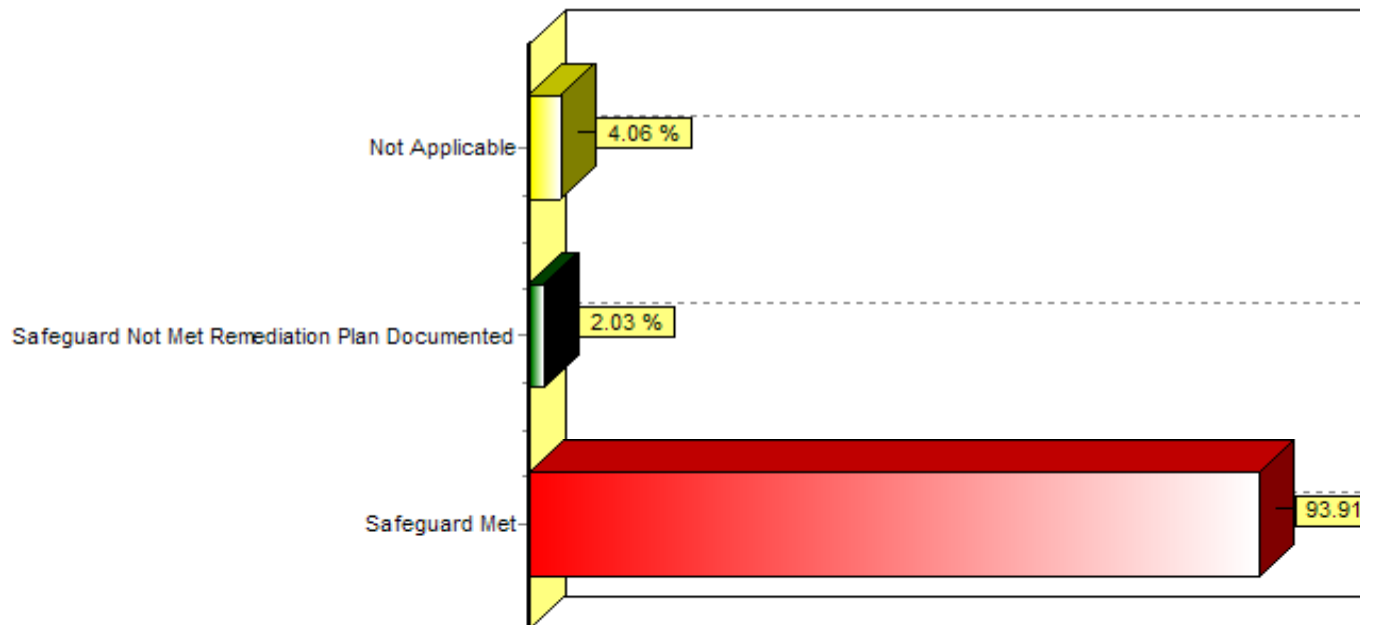
Bar Graphs

DHS Safeguards Assessment Tool 2005

F1. Approved DHS contractor performs removal and destruction of confidential materials.



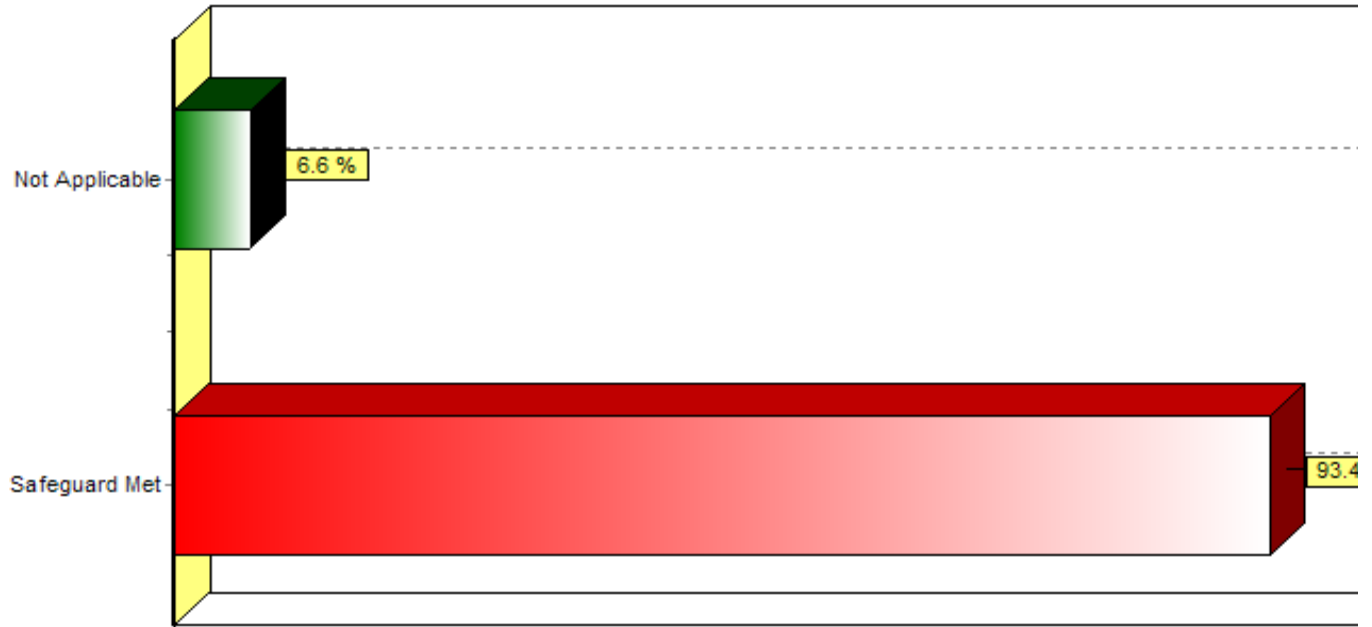
F2. Confidential material collected for disposal is placed in properly labeled containers. Container is labeled confidential and covered to prevent casual viewing.



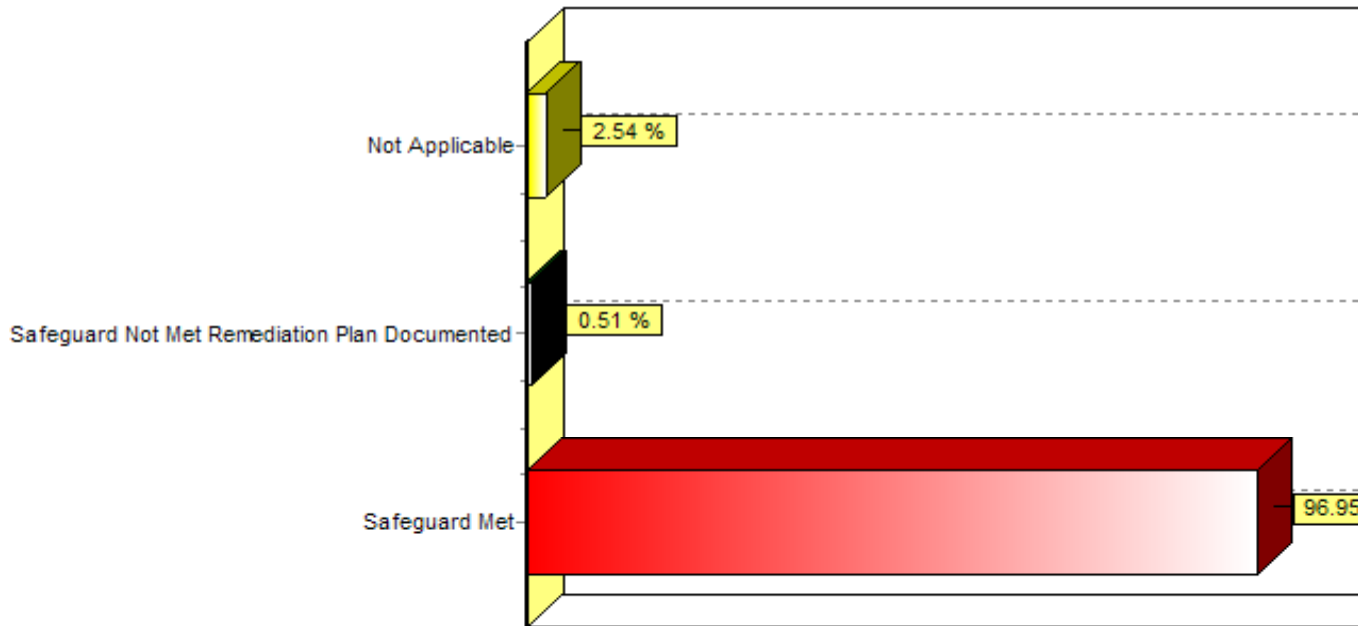
Bar Graphs

DHS Safeguards Assessment Tool 2005

F3. Confidential material waiting for disposal is placed in a designated secure storage area, or reasonable procedures are in place to minimize access if a secured storage area is not available.



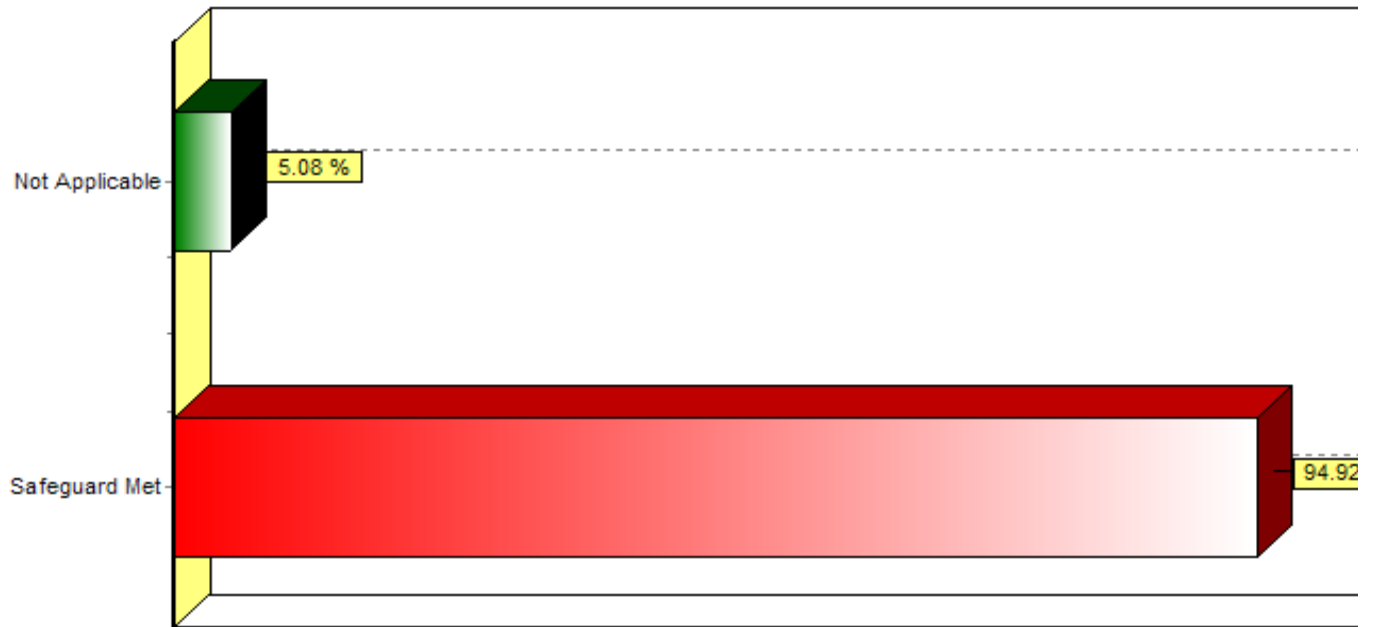
F4. Confidential material is not placed within common or desk waste paper baskets.



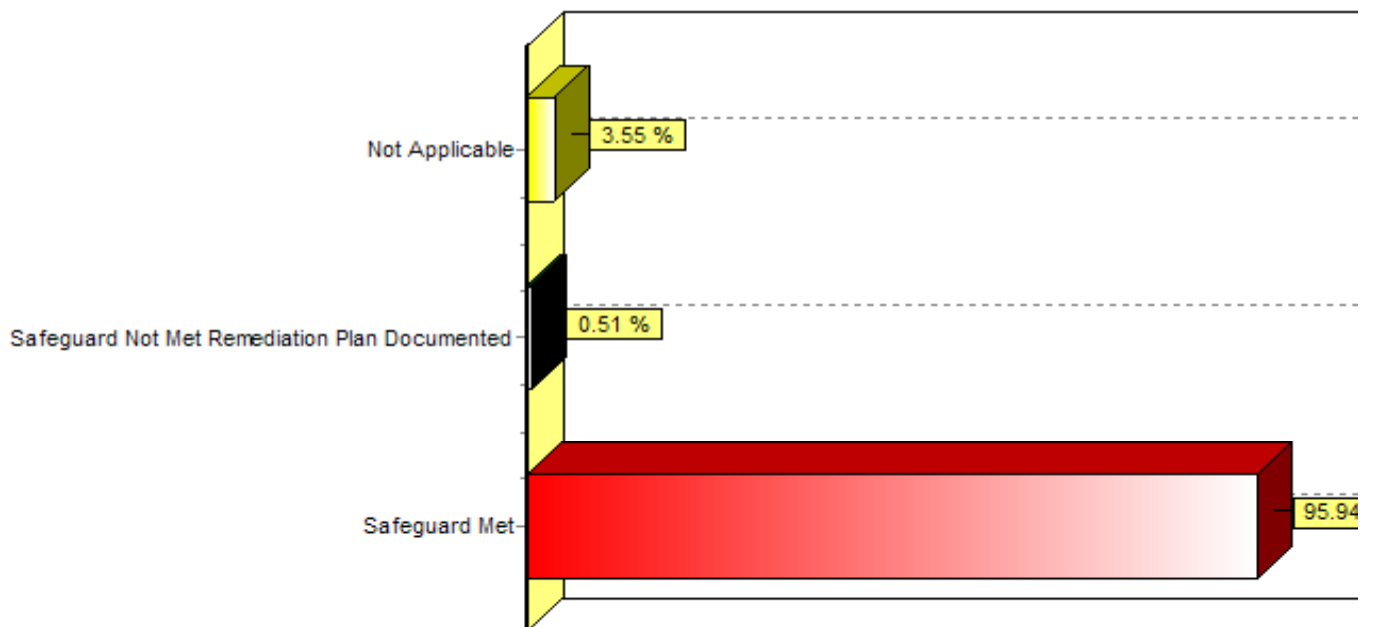
Bar Graphs

DHS Safeguards Assessment Tool 2005

F5. Shredding of files and documents is consistent with DHS record retention requirements and/or unit policy.



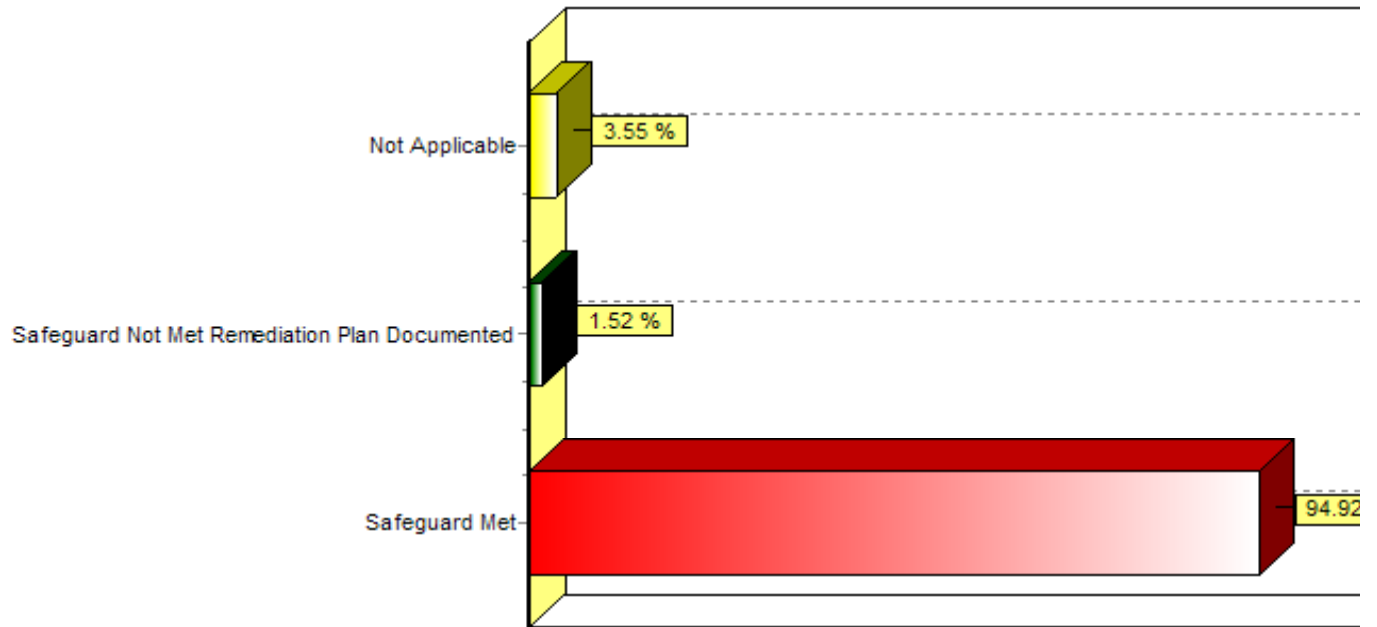
G1. Managers include building privacy/security practices in new employee orientation.



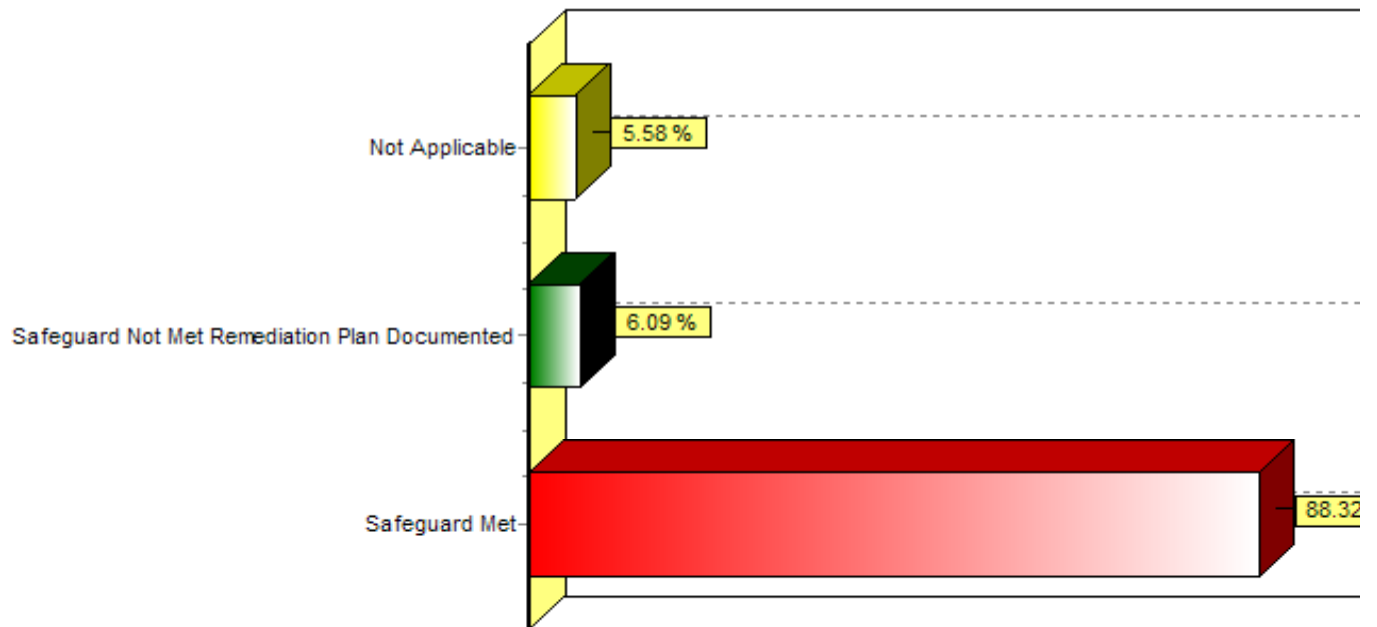
Bar Graphs

DHS Safeguards Assessment Tool 2005

G2. DHS managers or their designees conduct periodic internal reviews of site compliance with confidentiality practices and policies.



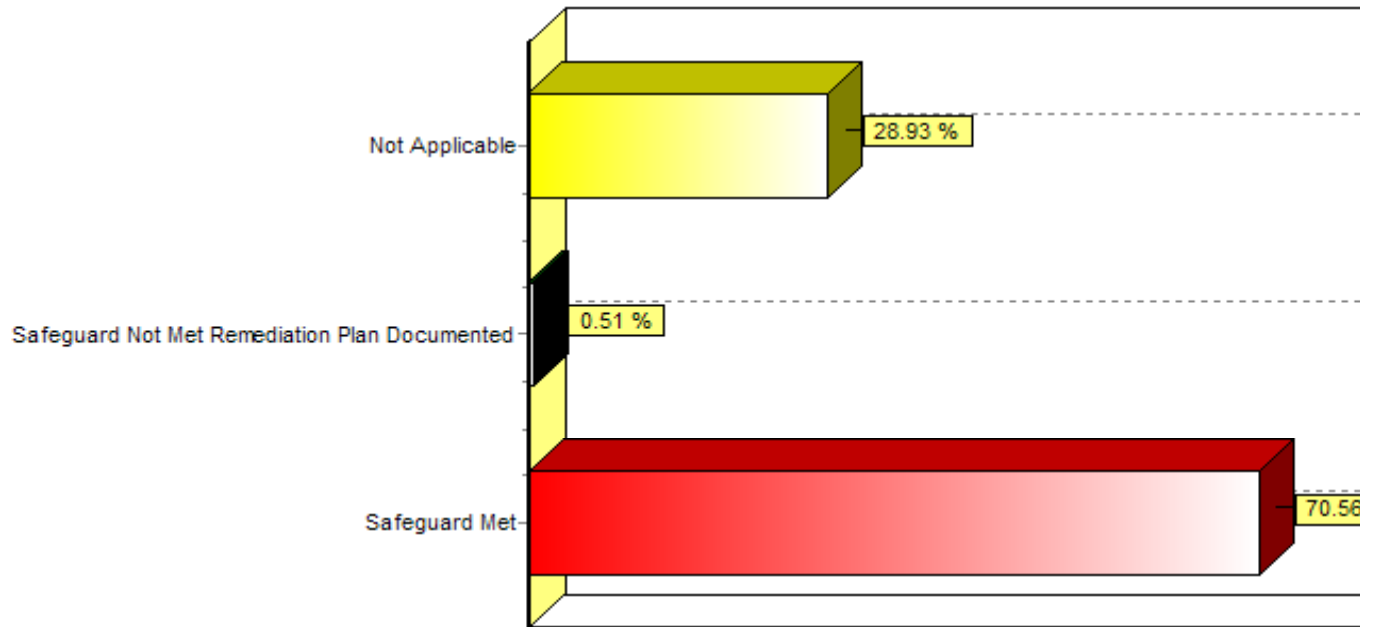
G3. At a minimum of once per year, managers review systems access for staff members, in order to ensure that appropriate access is added, maintained, or revoked.



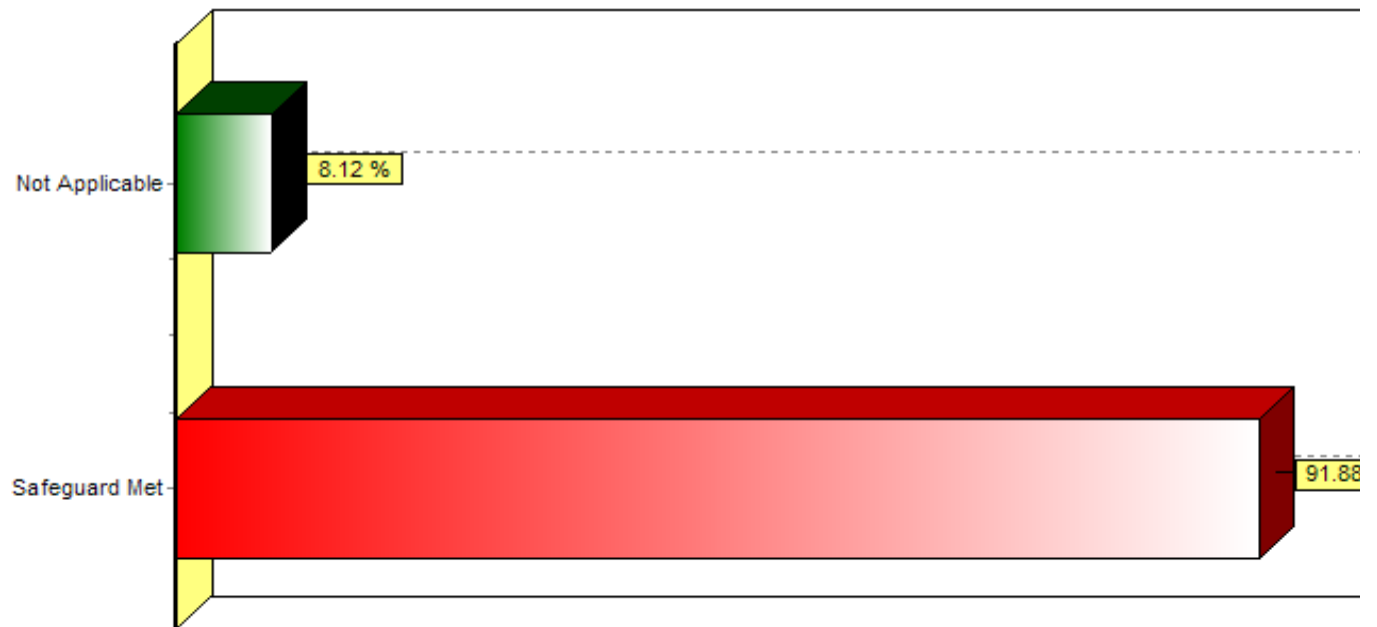
Bar Graphs

DHS Safeguards Assessment Tool 2005

G4. Non-DHS staff stationed in shared facilities are covered by a confidentiality agreement or are physically separated from areas where DHS staff discuss confidential information.



G5. Staff complies with office procedures regarding confidential information taken off-site in personal or state vehicles.



Bar Graphs

DHS Safeguards Assessment Tool 2005

G6. DHS managers ensure that staff members under their supervision are aware of privacy and information security policies, procedures, and guidelines, and have access to current versions.

