CIP Plan Review

I did a quick scan of the CIP document, and (skipping over readability/grammatical issues), here were the items I came up with:

- In general, the document talks a lot about what the department will do to determine their critical infrastructure, rather than talking of how they will protect it. Section 3 in particular is filled with future tense of how they will use Project Matrix to determine critical assets. Given that they now possess the surveys and (I presume) the subsequent results, I'd suggest rewriting the section to talk about the identified critical assets, instead of the plan to identify them. Otherwise actual protection is squeezed into sections 4 and 5, which only take up a third of the document (and even that consist mostly of plans).
- Also in general, this document seems more focused on the short term of creating and establishing the CIP plan rather than the CIP plan itself. Why include the project plan in Appendix E? Why even bring up Project Matrix, except as background? Understood that this is a work in progress, and that they want to revise the December 2000 plan per the biannual schedule. I would think that the idea behind this document would be how the CIP program works in perpetuity, not just for the next year and a half. Instead of due dates, perhaps use periodicity schedules, etc.

More specific:

- p.10 - for POs, it indicates that POs will designate a "single person within the PO responsible for their PO's critical infrastructure protection efforts, directly reporting to their Senior Officer." Who is that/have they already been identified(Andy, Mary, Ganesh)?
- p.10 - for Contractors, add that they are responsible for fulfilling security requirements *as per the conditions set within their contracts.*
- Kill off Figure 1-1 on p. 11; it's completely useless.
- p.14 - In the first paragraph, they define critical assets as assets whose "incapacitation could jeopardize national security..." etc. Seeing as how that's not applicable at ED, why bring up that definition? Provide the definition that Ed is using.
- p.14 - last paragraph sounds like a sales pitch for Project Matrix. Drop it.
- p.16 - As mentioned earlier, instead of writing about the planned approach for identifying critical infrastructure, simply identify the items and how it was done. Per the schedule, all the activities should have been completed.
- p.20/21 - Per the schedules, threat analyses and vulnerability assessments for POs' systems will take place at the end of this year/early next year. Shouldn't these have been part of the risk assessments? At the very least, the timeline they propose is counter to the very process they give. Per the graphic on p.22, threat analysis and vulnerability identification has to take place before the risk assessment occurs; otherwise, how can you determine the risks to your systems?
- p.30 - Not quite sure why this section is included. Seems to be a catch basin for items that didn't quite fit in other sections.
- Appendix A/G - change name to FSA in Org chart (A-1) and POC list (G-1). Also, update whomever will replace David Moore in the POC list.
- Appendix B - are all these actually applicable to CIP, or is this just a laundry list of any possible security regulations and documents?
- Appendix C - I assume this is TBD until after the CIP questionnaire is completed - it should be titled as such.
- Appendix E - as mentioned, why is this included?
- Appendix H - Include MEI in the list of acronyms.