```
-- global security parameters
security {
  -- adversary model for setup
  -- options: trusted-setup, no-trusted-setup
  trusted-setup
  -- adversary model for public key infrastructure
  -- options: pki, no-pki
  pki
  -- adversary model for behavior of corruptible parties
  -- This example says “at most 1 out of C and D are corruptible as semi-honest”
  -- options: semi-honest, semi-malicious, covert, malicious
  semi-honest
  corruptible: C,D <= 1
}

connected {
  -- broadcast capabilities
  -- options: broadcast, no-broadcast
  broadcast
  -- fully conntected parties
  full: A,B,C,D
  -- parties with communication links
  link: C-E,D-E
}

{-
below is secrurity-relevant information for each party

`ok-reveals` and `no-reveals` are coarse-grained approximations of the ideal
functionality

ok-reveals: a list of parties who can learn mpc results which compute over
            my data (a whitelist)

no-reveals: a list of parties who shouldn't learn mpc results which compute
            over my data (a blacklist)

If some party learns an mpc result and it is not listed in `ok-reveals` or
`no-reveals` then the possible flow is logged and reported, but the program is
not rejected. Programs are rejected if it is possible for an mpc result to be
revealed to a party on the `no-reveals` list.
-}

-- an input party, e.g., US NIST Agency
A {
  location: <US-NIST>     -- identify and digitcal location, for trust relationships and
communication
  ok-reveals: E           -- who am I ok with learning result of mpc which involved my
inputs
  no-reveals: B           -- who am I not ok with learning result of mpc which involved my
inputs
  encryption: 256         -- what strength of encryption needs to be used on my data
}
-- an input party, e.g., US DOE Agency
B {
  location: <US-DOE>
  ok-reveals: E
  no-reveals: A
  encryption: 512
}
```

```
-- a compute party: e.g., Amazon
C {
  location: <Amazon>
  no-reveals: all
}
-- a compute party: e.g., Microsoft
D {
  location: <Microsoft>
  no-reveals: all
}
-- an output party: e.g., US NSA
E {
  location: <US-NSA>
  no-reveals: all
}

{-
Any program that tries to read secret data from Amazon, Microsoft or US-NSA
will be rejected during compilation and never run, and security auditor of this
file can know this will always be the case, no matter what the program (or
ideal functionality) is. Also, a security auditor at US-NIST can know that
Amazon and Microsoft won't see any results from any MPC computation---only NSA
will---no matter what the program (or ideal functionality) is.
-}
```